

CUSTOMER AWARENESS - Do's AND DON'Ts ON ELECTRONIC BANKING TRANSACTIONS

DO's	DON'Ts
<ul style="list-style-type: none"> ➤ KEEP SECURE YOUR ATM DEBIT/ CREDIT CARD ➤ MEMORISE THE PIN OF YOUR ATM DEBIT & CREDIT CARD ➤ CHANGE THE PIN/ INTERNET BANKING PASS WORD FREQUENTLY ➤ BE CAREFUL WHEN YOU ARE DOING TRANSACTIONS AT ATM CENTERS - SEE ANY EXTRA FITTINGS ARE THERE OR ANY PERSON IS FOLLOWING YOU ➤ USE CANARA MSERVE APP TO SWITCH OFF ATM DEBIT / CREDIT CARD WHEN YOU ARE NOT USING ➤ CHECK TRANSACTIONS IN YOUR ACCOUNT REGULARLY AND INFORM THE BANK IF UNAUTHORISED TRANSACTIONS NOTICED ➤ REPORT UNAUTHORISED ELECTRONIC BANKING TRANSACTION AS EARLY AS POSSIBLE THROUGH ANY ONE OF THE FOLLOWING CHANNELS; <ul style="list-style-type: none"> A. CALL TOLL FREE NUMBER 1800 425 0018 B. REPORT THROUGH E-MAIL - reportsuspect@canarabank.com C. SMS TO 56161 BY TYPING SUSPECT FOR DOMESTIC CUSTOMERS D. SMS TO "9980904040" BY TYPING WORD "SUSPECT" FOR NRI CUSTOMERS (PRODUCT CODE 103 & 104) E. LOG IN TO OUR WEBSITE WWW.CANARABANK.COM AND LODGE THE COMPLAINT IN "CANARA PUBLIC GRIEVANCE REDRESSAL SYSTEM (CPGRS)" F. REPORT THROUGH PHONE BANKING/ IVRS G. REPORT TO THE BASE BRANCH OVER PHONE OR E-MAIL ➤ KEEP YOUR MOBILE AND PC WITH UPDATED ANTI VIRUS SOLUTION ➤ REPORT TO CYBER CRIME POLICE/POLICE AUTHORITY 	<ul style="list-style-type: none"> ➤ DO NOT DISCLOSE YOUR ATM DEBIT CARD / CREDIT CARD NUMBER/PIN/CVV/OTP TO ANY PERSON ➤ DO NOT SHARE YOUR INTERNET BANKING USER ID / PASSWORD/ OTP ➤ NEVER RESPOND TO ANY TELEPHONE CALLS/ SMS/E- MAIL ASKING TO SHARE THE DETAILS OF YOUR CARD NUMBER ETC ➤ DO NOT HAND OVER YOUR DEBIT CARD/ CREDIT CARD TO ANY UNKNOWN PERSON/ SALES PERSON IN A SHOP / MERCHANT LOCATION BEYOND YOUR SIGHT ➤ DO NOT KEEP PIN/PASSWORD ALONG WITH THE ATM DEBIT CARD/ CREDIT CARD - MEMORISE IT ➤ AVOID CYBER CAFES FOR DOING INTERNET BANKING TRANSACTIONS