ATM CARD & PIN SECURITY TIPS

- Do not keep the PIN issued by the Bank together with your ATM Card.
- Change your PIN immediately when using your ATM Card for the first time and destroy any documents containing PIN information.
- Do not write down your PIN. You should memorize it.
- Do not send your PIN via email/SMS and never use the same PIN to access other services.
- Do not write down your PIN on the card face and do not disclose your PIN to anyone including any joint account holder.
- Do not, under any circumstances, disclose your PIN to anyone who claims to represent the Bank or who claims to be the Bank's employee or other authorised person, or the police. It is not necessary for anyone to know your PIN. The Bank will never ask for your PIN by any means such as email, SMS, phone, or any other method etc.
- Do not use combinations that are readily accessible/deducible such as your identity card number, telephone number, date of birth, driver's license number or any popular number sequence (such as 987654 or 123456) for your PIN. Avoid using the same digit consecutively or the same sequence of numbers more than twice (such as 112233 or 383838) as a PIN.
- For security reasons, change your PIN regularly.
- If you enter an incorrect PIN several times (3 times) consecutively, the related service will be suspended. Please reset your PIN again at any branch to resume the service.

- Where possible, use ATMs with which you are most familiar. Alternatively, choose well-lit, well-placed ATMs where you feel comfortable
- Avoid using the ATM if it looks too isolated or unsafe.
- Survey your surroundings for any suspicious activity before withdrawing money.
- If anyone or anything appears to be suspicious, leave the area at once. If you drive to an ATM, park close to the terminal and observe the entire area from the safety of your car before getting out.
- Take another person with you to an ATM whenever possible, especially if at night.
- Avoid opening your purse, bag or wallet while in the queue for the ATM. Have your card ready in your hand before you approach the ATM.
- Notice if anything looks unusual or suspicious about the ATM indicating it might have been altered. If the ATM appears to have any attachments to the card slot or key pad, do not use it.

- Check for unusual instructions on the display screen and for suspicious blank screens. If you suspect that the ATM has been interfered with, proceed to another ATM and inform the bank.
- Be alert to your surroundings before conducting any banking transactions. Make sure no one sees your PIN and cover the keypad when you enter your PIN on any device, such as an ATM or other self-service terminal.

- Check that the protective keypad cover is intact before using any ATM. If in doubt, please notify the bank concerned immediately.
- Should you notice any suspicious devices at any ATM (such as micro-skimmers, pin-hole cameras, or fake key pads) or any suspicious activities around you when performing an ATM transaction, cancel your transaction immediately and inform the Bank.
- When you have completed your ATM transaction, please retrieve your ATM Card as instructed on the ATM. Never try pushing your card back into the ATM.
- Remember to take your cash and ATM Card after each ATM cash withdrawal.
- Count the banknotes immediately after each cash withdrawal. Keep all transaction receipts and check them against your account records.
- Do not take away any banknotes at the cash dispenser or ATM card at the card insertion slot left behind by someone else. Let the banknotes or ATM card return to the ATM automatically.
- Do not request someone else to perform ATM or other transactions for you.
- Do not accept assistance from strangers. If you encounter any problems at the ATM, contact the Bank directly.
- Shred anything that contain your credit card number written on it
- Check your bank balance and transaction history regularly. Call the Bank immediately of any actual or suspected unauthorised use of your ATM Card and/or PIN and confirm notification to the Bank in writing.
- If you are prompted to enter your PIN twice, or if you notice unusual messages on the screen, go to another ATM. However, if there is a time out or if the transaction is canceled and you enter your PIN a second time, check your statement to be sure the transaction does not appear twice.
- Prevent "shoulder surfing" by standing between the ATM and anyone waiting to use the terminal. Shield the keypad as necessary when entering your PIN and transaction amount.

  - Do not allow anyone to distract you while you are at ATM.
  - Never let a stranger assist you with an ATM.
  - Never Force your card into the card slot.
  - Minimize time spent at the ATM when conducting a transaction.

- When your transaction is complete, put your card, money and receipt away and immediately leave the area. Do not count your money while at the ATM.
- If for any reason your card is not returned to you by the ATM, contact your bank immediately. Follow the instructions on the display screen, e.g. do not key in your PIN until the ATM requests you to do so.
- If you are followed after using ATM, seek a place with people, activity and security.
- If your ATM card/PIN is lost or stolen or if someone else learns your PIN, please inform us immediately by visiting any branch, logging in to our mail atm@sawjibank.com or calling our hotline:02241561111/22

Using ATMs Abroad

- Verify your balances to make sure you have enough money in your account to cover your trip expenses to avoid running out of cash overseas.
- It's important to have a back-up plan in case your card is lost, stolen or held by ATM. It could be in the form of a second ATM card from a different issuer, cash, credit cards or traveler's cheques. Notify the bank beforehand and get a note added to your account so it does not get passed through the fraud section due to sudden change in account activity.
- Get international ATM support specifically activated for your ATM / debit card.
- Ask your bank for a contact number that you can call from overseas in case of need.
- Many ATMs abroad don't accept PIN longer than four digits. If your PIN is longer, change it.
- Foreign ATMs often don't have "0" (zero) digit button. So, make sure to change your PIN before leaving for abroad.
- Ask about overseas transaction and currency conversion fees.
- Banks charge either flat rate or a percentage of withdrawal amounts as transaction fee. Check with your bank before going abroad.
- ATMs have daily withdrawal limits which may or may not match those imposed by your bank. Ask about your bank limits and remember to plan it ahead in case you encounter lower withdrawal limits on your trip.
- At the time of payment, always check your receipt to ensure that transaction is not involving your home currency in a country that doesn't use that currency. Ask the merchant to re-do the transaction in the local currency and immediately report the incident to your credit card issuer.
- Foreign currency transaction fees will be charged if the merchant uses a foreign bank, even if the transaction is made in your home or local currency.

Protection of Card

- Ensure to sign the signature panel of your card as soon as you receive it.
- Treat your card like cash and ensure safe keeping of your card all the times.
- Cards are sensitive to mechanical, electromagnetic and sun impacts. Shield your card properly.
- Be aware of the expiry date on your card.

<u>Beware of following security threats:-</u>

- **Identity theft**

  The fraudulent acquisition and use of person's private identifying information, usually for financial gain. It can be divided into two broad categories:

- **Application fraud**

  Application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information.

- **Account takeover**

  Account takeover happens when a criminal tries to take over another person's account, first by gathering information about the intended victim, and then contacting their card issuer while impersonating the genuine cardholder, and asking for the mail to be redirected to a new address. The criminal then reports the card loss and asks for a replacement to be sent.

- **Phishing**

  Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

- **Skimming**

  Skimming is the theft of credit card / Debit card information. Thief can procure victim's credit card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victim's credit card numbers. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card and makes note of card details for further use.

- **Vishing**

  It is one of the methods of social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and "phishing".

- **Social Engineering**

  Social engineering involves gaining trust – hence the fraudster poses as a member of staff or even security guard. The fraudster would then ask the customer to check the card for damages.

  The fraudster would have gained confidence from his prey using various tactics such as offering assistance to the customer who perhaps would have tried to use the ATM without success or perhaps the customer who is not familiar with use of ATM machine and requires assistance

- **ATM & DEBIT CARD USAGE INSTRUCTION**

To enjoy the many conveniences ATM/Debit card offer, you are advised to follow some important safety tips: