OFFICE OF THE JOINT DIRECTOR (IT)
ROOM NO.7001, 7th FLOOR, PALIKA KENDRA
SANSAD MARG, NEW DELHI-110001
Office Telephone: 011- 415013673 Ext. 2240

ADVISORY FOR DO`S & DON`TS FOR ATM OPERATIONS

No.3/4659 /Jt.Dir (IT)/2020 Dated: 19/2/2020

It has come to the notice of IT Department that recently ATM fraud and clonning has been happened with NDMC Employess The following Do's and Don'ts help to remind us all of actions we must take to remain vigilant.

1. Card Skimmer

A card skimmer is a device which is designed to steal information from a card with magnetic strip, classically a credit card, when the card is used in a legitimate financial transaction. Once collected on the device, the skimmer can be used to make a clone of the card which can be used for fraudulent purposes, or the collected.

a) Some skimmers are designed as standalone units through which a card is swiped. For example, an unscrupulous restaurant/petrol pump employee might carry a skimmer so that he or she can run a customer's credit card and then run the card through the skimmer to collect the information. This type of skimmer can usually store numerous credit card numbers.

b) The second type of skimmer is a small electronic device which attaches to a credit card terminal or automated teller machine ATM). In this case, every time a card is swiped or inserted, the skimmer gathers the user's information, and it may be attached to a device which logs keystrokes to collect the personal identity numbers (PINs) of people who use the terminal

2. Always pay close attention to the ATM and your surroundings.

Don't select an ATM at the corner of a building—corners create a blind spot. Use an ATM located near the center of a building. Do your automated banking in a public, well-lighted location that is free of shrubbery and decorative partitions or dividers.Maintain an awareness of your surroundings throughout the entire transaction.

3. Be Aware

a) Be aware of people trying to help you with ATM transactions. Be aware of anyone sitting in parked car nearby. When leaving an ATM make sure you are not being followed. If you are, drive immediately to a police or fire station, or to a crowded, well-lighted location or business.

b) Memorize your PIN; never write it on the back of your card.

c) Do not re-enter your PIN if the ATM eats your card contact a bank official.Do not wear expensive jewelry or take other valuables to the ATM. This is an added incentive to the assailant.

d) Beware of "Shoulder Surfing" and Shield your PIN from onlooker by covering the keypad while entering the PIN.

e) Always change the PIN as soon as you receive it. Preferably, change it every quarter.Ensure to collect your Debit card, after completion of the transaction. Periodically verify the passbook entries to ensure its correctness. Any unauthorized card transaction in the account, if observed, should be immediately reported to the Bank.

f) Please ensure that the card is swiped in your presence at POS terminal (Point of Sale).

g) After completion of your transaction and before leaving the premises please ensure that 'Welcome Screen' is displayed in the ATM/Cash deposit machine

h) Do not leave your statements that are printed after a transaction behind. Take it home and shred them.

i) Never count cash at machine or in public. Wait until you are in your car or another secure place.

A.W. Ansari
Joint Director(IT)

Copy to:

1. PS to Chairman for information please.
2. PS to Secretary for information please
3. PS to Financial Advisor for information please
4. PA to Director (IT) for information please
5. Head of Departments
6. Notice Board`