इण्डियन ओवरसीज़ बैंक **INDIAN OVERSEAS BANK**

Skimming

Dear Customer,

Greetings from IOB

Skimming a method used by criminals to capture data from the magnetic stripe on the back of Debit/Credit card. Skimming of credit/debit card data is performed at point of sale (POS) and ATMs.

How a Skimming device look like?

Skimming Device: The card reader slot is fixed with a cover piece that mirrors the existing reader piece on the machine. This is affixed with tape and will come off if rotated or pulled on.

The pinhole camera device which captures the customers pin number as it is entered. This is affixed with tape or glue. It can be removed by pulling it downward

Fake Keypad to capture PIN

Tips to protect against skimming

✓ Examine the ATM /POS terminal for any suspicious object before usage.	✓ Never share your PIN.
✓ Change your PIN regularly	✓ Check your account regularly.
✓ Choose PIN difficult to guess (e.g. Avoid Birthdate, Phone, Car numbers)	✓ Cover the keypad with your hand when entering PIN.
✓ ATM at branch, inside the mall, is generally safer than a lone outdoor ATM. Choose ATMs that are in well-lit, public or highly populated areas.	✓ Immediately call your bank if you suspect your account/card has been compromised.

With warm regards,
Chief Information Security Officer
Indian Overseas Bank, Central Office, Chennai