



External Relations Department

ERD/M&PRD/PR/01/2017-111

December 5, 2017

SBP takes notice of skimming incidences—relevant Bank to compensate fully its customers.

During the preceding week, State Bank of Pakistan noted with concern that customers' information on debit cards of Habib Bank Limited was compromised by hackers through skimming to create its clones and were used to withdraw depositor's money from various locations within and outside the country. Since then SBP has been in contact with HBL management to ascertain the losses, returning of money to the affected customers and precautionary measures to limit the impact of this hacking activity.

HBL has taken several immediate actions to determine and limit the impact of such transactions on customers. Specifically, it blocked all identified debit cards that were suspected to be misused and quarantined the Automated Teller Machines (ATM) used in hacking activity. Till today, 296 customers have confirmed the disputed transactions and the estimated damage assessment done to the concerned Bank is Rs10.2 million for their customers. HBL has also managed to start returning the money to depositors to the extent of their losses. Meanwhile efforts are underway to determine losses to any other bank's customers using HBL ATMs and take remedial measures.

ATM skimming — an illegal activity in which account details are stolen from the magnetic strip contained on the back of the debit card has been around for a while and such incidents have happened, sporadically, in Pakistan as well. To safeguard the depositors from fraudulent transactions, SBP has issued specific regulations for the security of payment cards and internet banking, under which banks are required to develop and implement comprehensive framework for risk assessment, implementation of controls and monitoring.

It would be pertinent to mention here that debit cards with a magnetic strip on its back – that stores customer's account details are particularly vulnerable to skimming and cloning. Debit cards, complying with EMV (Europay Mastercard Visa) standards, featuring a chip and offering two factor authentication are now considered most effective countermeasure for card cloning through skimming globally. Accordingly, SBP vide its circular PSD 05 of 2016 issued regulations for Payment Cards Security wherein banks are required to develop infrastructure for EMV Compliance and issue cards by 30th June 2018.

SBP reassures bank's customers that complying with its responsibility of ensuring a smooth and safe payment systems it will take every measure in coordination with banks to safeguard the interest of depositors against any fraudulent activity.
