STATE BANK OF PAKISTAN
PAYMENT SYSTEMS DEPARTMENT
I. I. CHUNDRIGAR ROAD
KARACHI

PSD Circular No. 09 November 28, 2018

The Presidents/CEOs
All Banks/ MFBs

Dear Sir/ Madam,

Security of Digital Payments

In order to safeguard banks/MFBs and their customers from potential losses due to cyber-crimes and online banking frauds, it has been decided that:

i) Banks/MFBs shall immediately carryout extensive vulnerability assessment and penetration testing to identify potential weaknesses in their Alternate Delivery Channels (ADCs) and payment systems including but not limited to Card Systems, RTGS, SWIFT, Internet/mobile banking and agent-based/Branchless Banking etc. The assessment reports alongwith action plans and timelines to address the vulnerabilities shall be submitted to Payment Systems Department (PSD) latest by March 31, 2019.

ii) In addition to the internal assessments, banks/MFBs shall arrange independent 3rd party review/assessment of their Alternate Delivery Channels (ADCs) and payment systems including but not limited to Card Systems, RTGS, SWIFT, Internet/mobile banking and agent-based/Branchless Banking etc. These assessment reports shall be submitted to PSD latest by December 31, 2019.

iii) With effect from January 01, 2019, Banks/MFBs shall send free of cost transaction alerts to their customers through both SMS and email (*where email IDs are available*) for all international and domestic digital transactions including but not limited to ATM, POS and Internet banking transactions. Such transaction alerts shall be generated and relayed to customers immediately after the execution of transaction. For this purpose, registered mobile phone numbers and valid email addresses (*where applicable*) of all customers shall be obtained, verified and updated in the bank/MFB's database well before the deadline.

iv) Henceforth, banks/MFBs shall activate/reactivate online banking services including internet/mobile banking for their customers after biometric verification at any branch of their bank. At the time of activation of online services, banks'/MFBs' relevant staff shall educate customers about various types of online banking frauds as well as the corresponding preventive measures. Banks/MFBs shall be solely responsible for ensuring customer authentication for activation of any ADC and any loss of customer funds due to false activation of any ADCs shall be compensated by the respective bank/MFB.

v) All card-issuing banks/MFBs shall acquire/upgrade the capability to enable their customers to activate or block their cards for online/cross-border transactions as and when required by them latest by March 31, 2019.

vi) With reference to PSD Circular No. 05 of 2016, all card-issuing banks/MFBs shall replace all existing payment cards (*except social transfer cards*) with EMV chip-and-PIN payment cards latest by June 30, 2019.

vii) All card issuing/acquiring banks/MFBs shall deploy real-time fraud monitoring tools and alert mechanisms, preferably provided by their Payment Schemes, to detect potential fraudulent activities on their Card Systems latest by January 31, 2019. Further, card-issuing/acquiring banks/MFBs shall develop Standard Operating Procedures (SOPs) for threat reporting and escalation as well as actions to be taken in case suspicious activity is reported or identified.

viii) Banks/MFBs shall make arrangements to monitor on 24/7 basis usage/activity regarding payments made through their cards or through online transactions on their internet banking platforms. Banks/MFBs shall have arrangements in place to immediately contact (through multiple communication channels) and coordinate with designated people of Payment Schemes for taking appropriate action in case any abnormality in transaction patterns is observed.

ix) Banks/MFBs shall immediately review their existing agreements with Payment Schemes to identify clauses that may expose them to potential financial, legal and operational risks arising due to cyber-attacks/crimes and take appropriate risk mitigation measures with the approval of their Board/senior management.

x) All payment-card issuing banks/MFBs shall immediately set reasonable per-day transaction limits commensurate with their risk appetite and transaction volume with the Payment Schemes especially for cross-border usage. Banks/MFBs shall ensure that their risk exposure remains within the pre-agreed limits set with the international/domestic payment schemes through legally binding contractual arrangements.

xi) It has been observed that Payment Schemes usually issue advisories to member banks regarding steps to be taken after a security breach incident is reported. However, some banks/MFBs do not take timely actions on these instructions thus exposing themselves to various risks. In this regard, banks/MFBs are advised to take full coverage of Payment Schemes' cybersecurity threat intelligence and advisories including update of indicators of compromise (IOCs) and ensure immediate compliance with preventive actions advised by the Payment Schemes from time to time. A detailed log of such advisories and the actions taken shall be maintained and properly audited.

xii) Banks/MFBs, in consultation with Payment Schemes and third-party technology service providers shall make arrangements to ensure that latest security patches are installed on their digital payments infrastructure including customer touchpoints like ATMs and POS machines etc. as soon as they are released.

xiii) To prevent frauds in online transactions, banks/MFBs shall enable EMVCo's 3D Secure Security Protocol. A detailed plan for the implementation of EMVCo 3-D Secure for all applicable card payments shall be submitted to PSD latest by January 31, 2019.

xiv) Banks/MFBs shall start assessing the feasibility of implementing Payment Card Industry Data Security Standards (PCI DSS) and Payment Application Data Security Standard (PA DSS) for their digital payment systems and adoption of the same standards by their third-party technology service providers. Banks/MFBs shall submit their assessment reports in this regard to PSD latest by January 31, 2019.

xv) Acquiring banks/MFBs shall educate their POS retailers as well as their employees regarding risks of theft of customer's card data at POS terminals as well as mechanism to monitor such risks. Further, the acquirer banks/MFBs shall discourage the practice of card swiping at merchant's non-POS terminals especially when the merchant is not PCI DSS compliant.

xvi) Banks/MFBs shall continuously educate their customers using print, electronic and social media about prevalent banking frauds including but not limited to call and SMS spoofing, impersonation by fraudsters etc. Specifically, customers shall be made aware that the banks/MFBs will never ask about personal information on phone or by email and that they would be liable for any financial losses in case they share their personal credentials with anyone when approached by the person(s) claiming to belong to bank's staff, law enforcement agencies, SBP, Benazir Income Support Program (BISP) etc.

xvii) In case, if it comes to the knowledge of any bank/MFB that their customers' data has been compromised, they shall immediately take steps to protect their customers from further losses and inform them within 48 hours about the steps being taken by the bank/MFB in this regard. In case of a financial loss to customers due to such incidents, the bank/MFB shall compensate them within two (02) business days. Further, banks/MFBs shall report such incidents to the Banking Policy & Regulations Department (BPRD) within 48 hours as stipulated in BPRD Circular No. 05 of 2017 on Enterprise Technology Governance & Risk Management Framework for Financial Institutions.

2. In addition to the above instructions, banks/MFBs shall ensure meticulous compliance of SBP's instructions with regard to safety and security of digital transactions; especially PSD Circular No. 3 of 2015 and PSD Circular No. 5 of 2016 and submit a fortnightly progress report to PSD. Failure to comply with the above instructions will lead to penal action by SBP including but not limited to the suspension of non-compliant digital payment products and services of the banks/MFBs.

Please acknowledge receipt.

Yours sincerely

(**Syed Sohail Javaad**)
Director