Frequently Asked Questions (FAQs) on PSD Circular No. 09 of 2018 – Security of Digital Payments

Issued vide PSD Circular Letter No. 01 of 2019

Payment Systems Department

Clause (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.

FAQs on Clause (ii)

1. **What banks are required to do as per this clause?**
   Answer: Banks are required to perform full-scale vulnerability assessment and penetration testing of their digital infrastructure with the objective to identify potential and inherent weaknesses in their technology platforms.

   Banks shall engage independent 3rd party assessors to perform a holistic review/assessment of their digital payment infrastructure including but not limited to compromise assessment to identify already compromised systems/platforms and software applications etc.

Clause (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.

FAQs on Clause (iii)

1. **How will this requirement be implemented?**
   Answer: With effect from January 01, 2019, banks/MFBs are required to send free transaction alerts for every transaction performed using digital channels including but not limited to ATM, POS and internet banking etc. within and outside Pakistan.

   Implementation of this clause would require provisioning of free of cost SMS and email alert services to all existing/future customers who subscribe to electronic/digital banking services including but not limited to ATM, POS and Internet banking transactions either locally or internationally. Banks/MFBs who have already charged fee from customers for such transaction alerts shall revert the same.

   In addition, banks/MFBs can offer their customers paid SMS alert services for other in-branch transactions only if the customers so desire. For all such transaction, banks/MFBs shall follow relevant legal/regulatory instructions alongwith proper disclosure and consent of the customer.

Frequently Asked Questions (FAQs) on PSD Circular No. 09 of 2018 – Security of Digital Payments

Issued vide PSD Circular Letter No. 01 of 2019

Payment Systems Department

Clause (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.

FAQs on Clause (iv)

1. **How will this requirement be implemented as internet banking involves a number of different type of transactions including fund transfers, bill payment, balance inquiry etc.?**
   Answer: Banks can activate online banking facility as per the existing practice; however, Intra-bank and Inter Bank Fund Transfer (IBFT) functionality through online banking including fund transfer to mobile wallets and mobile top-ups shall be activated for customers only after biometric verification.

2. **Can activation be done only through branches or offsite activation is also allowed?**
   Answer: For customer facilitation, authorized staff of Banks/MFBs may perform offsite customer biometric verification as well while ensuring safety, security and integrity of customer credentials.

3. **Is this requirement also applicable on branchless banking (BB) accounts?**
   Answer: The requirement mentioned in Question 1 above, shall not be applicable on Branchless Banking accounts which will continue to be regulated as per the requirements of Branchless Banking Regulations as issued and amended from time to time.

4. **What does reactivation mean in this clause?**
   Answer: By 'reactivation', the clause refers to the process of reactivating internet banking services of a customer whose services are blocked due to any reason. For example, a customer is using internet banking services but his/her account becomes dormant due to non-usage for any reason thereby his/her internet banking services are blocked. Once the account is activated upon customer's request, his/her internet banking services shall only be reactivated subject to biometric verification.

5. **How would this clause be implemented in case of customers being foreign nationals or in cases where customers biometric is illegible due to any reason?**
   Answer: In case of foreign nationals and citizens with illegible fingerprints, the traditional procedure for activation of online banking may be used with enhanced due diligence measures in line with BPRD instructions issued vide BPRD Circular Letter No. 16 of 2018 and BPRD Circular Letter No. 20 of 2017.

6. **For Non-resident Pakistanis (NRPs) and residents temporarily outside Pakistan, how would this clause be implemented?**
   Answer: In case of NRPs and Resident Pakistanis temporarily outside Pakistan, Banks may use the verification procedures defined vide BPRD Circular Letter No. 16 of 2019, for activation of online banking services.

Clause (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.

FAQs on Clause (v)

7. **Does this mean banks have to block all existing cards for online/cross-border transactions?**
   Answer: As per PSD Circular No. 05 of 2016, bank/MFBs shall take consumer consent regarding the utilization of Payment Cards on various ADCs or their cross border usage while maintaining the record of consent as per SBP record retention policy. However, it is observed that few banks do not have systems/capability to activate/block payment cards for online/cross-border usage as required by customers. Therefore, as per this clause, banks/MFBs are required to acquire/upgrade their existing systems, latest by March 31, 2019, to be able to activate and/or block usage of cards for online and cross-border transactions upon customer's request in order to achieve compliance with PSD Circular No. 05 of 2016.

Clause (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.

FAQs on Clause (xii)

1. **The clause seems to be in conflict with Section 3.4 of SBP BPRD Circular No. 05 of 2017 on Enterprise Technology Governance & Risk Management Framework for Financial Institutions.**

   Answer: The above-referred clause requires installation of latest security patches by banks/MFBs on their digital payment infrastructure. However, the installation of such patches shall be in line with banks/MFBs' establish procedures as required in Section 3.4 of SBP BPRD Circular No. 05 of 2017 on Enterprise Technology Governance & Risk Management Framework for Financial Institutions.

Clause (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.

FAQs on Clause (xvii)

1. **The two (02) days timeline to compensate the customers in case of a financial loss is not practical.**

   Answer: The two (02) days timeline to compensate customers who suffer a financial loss in case of a compromise of banks' systems refers to two (02) business days after the bank has established that the customer data has been compromised and caused a financial loss to the customers.