19th January 2024

Guidance Note – Effective controls to mitigate frauds and other losses due to Operational lapses

A recent incident in one of the Banks in India underscored vulnerabilities wherein users exploited incorrect responses triggered by the bank, resulting in wrongful credits leading to misuse by the customers by way of cash withdrawals and fund transfers. These breaches can be attributed to multiple systemic and process failures across various functions of the bank.

To strengthen controls and processes within the banking ecosystem, it is important to reiterate and adhere to the best practices across functions. The recommendations provided are generic in nature and are not specific to any particular payment product; however, it is important that these are implemented comprehensively to avoid financial and reputational losses.

Operational Controls

Banks should put in place a mechanism to monitor abnormal variations in key portfolio parameters from an issuing and acquiring perspective. This includes real time and batch monitoring of critical parameters to identify issues early. Some of the key parameters include:

- Steep increase in Business Declines, Technical declines and identify reasons for the same.
- Steep increase or decrease in daily/weekly/monthly variances in volume/value.
- Track refund/reversals as a % of the overall volume/value and also look for increase in absolute numbers.
- Track the overall count & value of Chargebacks raised/received and compare it with average/peak numbers noticed in the past and ascertain reason for the same.
- Monitor the accounts with high chargebacks and ascertain the genuineness of the customers raising such high chargebacks.
- Track steep increase or decrease in parameters such as ‘Deemed acceptance’, fallback, autopay, international volumes, overall transactions etc.
- Carry out reconciliation immediately after completion of a settlement cycle. It is recommended that the reconciliation is done multiple times a day depending upon the number of settlement cycles.
- Carry out 3 way reconciliation i.e. clearing system data, switch data and the data of Core Banking System (CBS) to ensure all the transactions are processed and all eligible transactions are settled properly. The status of a transaction between the switch and the core banking should be same.

Fraud controls:

- Monitor accounts with huge funds flow however the balances at end of day is negligible
- Transaction monitoring is traditionally focussed on the remitter side (debit transaction). However, monitoring should also be done on Beneficiary side (transaction credit).
- Monitor unusual count of debits/credits from specific accounts as compared to previous average.
- Establish profiling at customer level and transaction level based on previous transactions and flag off deviations.
- Put in place dedicated transaction/fraud monitoring team to reach out to customers proactively on encountering suspicious patterns.
- Have a suitable fraud monitoring system with real time and near real time capabilities.
- It is important to build Artificial Intelligence/Machine Learning (AI/ML) capabilities in fraud monitoring, identification of mule accounts etc when dealing with huge volumes of transaction where typical rule-based approach will be ineffective.
- Effectively use NPCI's EFRM system to complement any existing fraud monitoring system used by the bank.
- Any anomaly/incident identified to be reported to NPCI immediately on the same day. The investigation may be simultaneously carried out and further updates can be shared at a later date once more clarity is received.
- Alerts from NPCI to be acted on priority as these are sent basis specific intelligence built at an ecosystem level.
- Such alerts, be it from NPCI or from other member banks should be give adequate importance and at least a 2-level review by sufficiently senior on-roll employees and response for such alerts should be sent promptly.
- Banks to immediately stop/temporarily suspend the operations/product offering when serious abnormalities are noticed so that exposures, if any can be curtailed.

Information Security Controls:

- Version control of the software should be strictly followed so that only the code that is tested for functionality as well as security compliance is used in production.
- Banks should maintain an up-to-date inventory of Assets (Servers, DBs, Network & Security devices, Software, laptops) including their business criticality.
- Implement strict access controls to limit user permissions and restrict access to sensitive functionalities and data.
- Banks should define and implement secure coding practices, addressing flaws, threats due to insecure coding.
- Banks should conduct Secure Configuration review, Vulnerability Assessment and Penetration testing. Observations should be closed within agreed and management approved timeline.
- Banks should perform Secure Code review and Application Security assessment including but not limited to OWASP and SANS-25 guidelines.
- Conduct regular code review and Firewall rule assessments to identify and address potential weaknesses in the application.
- Banks should use strong encryption mechanisms such as: AES (Advance Encryption Standard) 256 bits and above along with minimum channel encryption of TLS 1.2.
- Banks should have Secure Key and Secret Management process including but not limited to periodic key rotation, segregation of duties, secure storage, archival and deletion, revocation of compromised keys, logging, and auditing of key management activities.
- Establish comprehensive logging and monitoring systems to detect and respond to any suspicious or anomalous activities or changes done in production environment.
- Banks' BCP/DR capabilities for people, process and technology should adequately and effectively support the cyber resilience objectives designed to recover rapidly from cyber-attacks/other incidents and safely resume critical operations and should be aligned with recovery time objectives.
- Banks should perform DR drills for all critical applications at least Quarterly to ensure the resiliency of applications.
- Banks should backup the data and periodically in isolated environment preventing any lateral movement of malwares and should restore backed up data to check its usability.
- Banks should have appropriate environmental controls for securing location of critical assets providing protection from natural and man-made threats. Monitoring mechanism should be deployed for detection of any compromise.
- Appropriate physical security controls such as: Access control, Facility security, Asset protection, Emergency response capabilities should be deployed.
- Bank should have compliance with the regulatory norms published by RBI on November 07, 2023 under RBI/2023-24/107 DoS.CO.CSITEG/SEC.7/31.01.015/2023-24.

System Audits:

- Regularly conduct Process audits as agreed with Internal Audit. IS audit should be carried out at least on quarterly basis to check effectiveness of ITGC (IT and InfoSec General controls).
- Conduct annual audit of systems/security audits through a CERT-In empaneled auditor. (Refer Master Direction on Digital Payment Security Controls dated February 18, 2021 (RBI/2020-21/74 DoS.CO.CSITE.SEC. No.1852/31.01.015/2020-21)
- Ensure that third-party vendors involved in digital payments adhere to robust security standards to mitigate vulnerabilities. (Refer Master Direction on Outsourcing of Information Technology Services dated April 10, 2023 (RBI/2023-24/102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24)
- Develop a comprehensive incident response plan to efficiently handle and mitigate the impact of any security breaches.

****