Transaction Monitoring Prevention System (TMPS) under the State Bank of Pakistan (SBP) guidelines:

The features would typically focus on ensuring compliance with regulations and enhancing the ability of financial institutions to detect and prevent financial crimes. Here are some features that should be highlighted in the request:

- **Real-time Transaction Monitoring:** The system should be able to monitor and analyze transactions in real-time to detect any suspicious activity immediately.
- **Automated Suspicious Activity Alerts:** Automated alerts generated for transactions that meet predefined risk criteria, such as large transfers, unusual patterns, or transactions involving high-risk jurisdictions.
- **Risk-Based Profiling:** Customers and transactions should be risk-profiled using parameters like transaction history, geographical risk, transaction size, and type of account.
- **Audit Trail and Transaction History:** Maintain an immutable audit trail of all transactions and actions taken on suspicious transactions.
- **Data Security and Privacy Controls:** The system should include robust encryption, access controls, and data anonymization protocols to ensure that sensitive financial data is protected.
- **Integration with Existing Banking Systems:** The TMPS should integrate smoothly with the bank's existing core banking systems, databases, and other monitoring tools.
- **Scalability and Flexibility:** The system should be scalable to handle increasing transaction volumes and customizable to fit the bank's needs in future.
- **User-Friendly Interface:** An intuitive and easy-to-navigate user interface for efficiently monitor transactions, review alerts, and generate reports.

- Identify and implement digital fraud risk controls to continuously monitor, prevent, detect, respond and remediate incidents of fraud.

Enterprise Fraud Management System:

The objective of this procurement request is to acquire a state-of-the-art Enterprise Fraud Management System (EFMS) to enhance the capabilities of the bank in preventing, detecting, and managing fraud, in full alignment with the directives and compliance requirements set forth by the **State Bank of Pakistan (SBP)**.

The Enterprise Fraud Management System must comply with all SBP circulars, guidelines, and regulations relevant to fraud detection, reporting, and risk management. The system should meet SBP's requirements related to:

- **Data Security and Privacy**
- **Audit and Compliance:** The system must generate comprehensive audit trails and support SBP's compliance reporting requirements.
- **Operational Guidelines:** Must ensure continuous system monitoring, incident detection, and real-time alerts in accordance with SBP's operational instructions.
- **Fraud Prevention:** Establish a system that prevents unauthorized transactions, financial fraud, and cyber threats.
- **Real-Time Monitoring:** Implement real-time monitoring tools for instant detection and alerts for fraudulent activities. The system must leverage machine learning, AI, and rule-based analysis to detect fraudulent activities in real time.
- **Data Integration:** The system must be capable of integrating with the bank's branchless banking, core banking system and other relevant systems to ensure seamless data flow and fraud detection.
- **Auditability:** Provide comprehensive, detailed, and verifiable audit logs for all system transactions and actions.
- **User Interface:** An intuitive, user-friendly interface with customizable dashboards for fraud monitoring and reporting.
- **Fraud Detection:** The system must provide advanced fraud detection mechanisms that are capable of identifying and managing emerging fraud patterns.
- **Maintenance and Support:** Ongoing support and system updates in compliance with SBP's technical support requirements.

SBP Guidelines on EFM System:

FIs shall ensure continuous monitoring of the services extended to the customer for which FIs shall implement an Enterprise Fraud Management (EFM) solution that should support detection, analysis and management of fraud across users, accounts, products, processes and channels.

The scope of real-time fraud monitoring tools and alerts mechanism specified in the PSD Circular No. 09 of 2018 related to payment card systems shall be enhanced to include all digital products. Further, FIs shall implement fraud risk scenarios which shall be periodically reviewed, require additional authentication from the customers based on digital fraud risk score, and for taking timely actions such as suspending transactions/accounts, etc. For this purpose, FIs may use Intelligent Algorithm based Customer's Transaction Behavior Profiling techniques for detection of suspected transactions. Some fraud risk scenarios may include but not limited to:

a. Change of device followed by credential reset request;

b. Change of device followed by addition of number of beneficiaries and IBFT transactions;
c. Addition of multiple beneficiaries followed by multiple debit transactions not in line with the historical pattern;
d. Change of geographic region;
e. Value, number and time of transactions;
f. Deviation in mean time to carry out transactions;
g. Transfer of funds to accounts, suspected to be involved in fraudulent transactions;
h. Suspected IPs and geo locations;
i. Multiple transactions in quick succession.

Identification of the devices (e.g. mobile phones, computers, tablets, etc.) used to digitally access significant number of accounts (especially victims' accounts, layering accounts and fund utilization accounts) in order the take necessary action against such devices including blocking access of digital services through the device.