



Open Banking Regulations 2026

Payment Systems Policy &
Oversight Department

(Digital Financial Services
Group)

State Bank of Pakistan

Contents

1) Acronyms	3
2) Definitions	4
3) Introduction	5
4) Authority	5
5) Scope of Open Banking	5
5.1 Scope of Participation	5
5.2 Scope of Data and Accounts	5
5.3 Scope of Services.....	5
5.4 Raast as Centralized API Hub	6
6) Authorization of TPP	6
7) Consent and Authorization	7
8) Liability Architecture	8
8.1 Liability Provisions.....	8
8.2 Dispute Resolution Mechanism	9
9) Governance	9
10) Internal Control Systems.....	10
11) Customer Recourse Mechanism	10
12) AML/CFT/CPF Requirements	10
12.1. Mitigation of ML/TF/PF Risk	11
13) Data Protection, Security and Privacy.....	11
14) UI/UX Guidelines.....	12
15) Pricing of product and services.....	12
16) Compliance with Existing Regulatory Frameworks.....	12
Annexure-A – Rules for Customer Recourse Management	14
Annexure-B -Minimum Set of Documents required for Onboarding/Sign-up by TPPs	16



1) Acronyms

AHI	Account Holding Institution
AISP	Account Information Service Provider
AML/CFT/CPF	Anti-Money Laundering, Combating the Financing of Terrorism & Countering Proliferation Financing
API	Application Programming Interface
EMI	Electronic Money Institution
IBAN	International Bank Account Number
MFB	Microfinance Bank
OB	Open Banking
PISP	Payment Initiation Service Provider
PS&EFT Act, 2007	Payment Systems and Electronic Fund Transfers Act, 2007
PSO and PSP	Payment System Operator and Payment Service Provider
RPP	Raast Payments Pakistan
SBP	State Bank of Pakistan
TPPs	Third Party Providers
UI/UX	User Interface / User Experience

2) Definitions

- i. **Account** means current account, saving account, branchless banking accounts, e-money or any other type of account/wallet maintained by a customer for payments with an Account Holding Institutions (AHI)
- ii. **Account Holding Institution (AHI)** means banks, MFBs, and EMIs holding customer's accounts/wallets and related data.
- iii. **Account Information Service (AIS)** means a service of collecting customer data of one or more accounts held by a customer with AHI(s) and consolidating, organizing and presenting such information to the customer in an easily understandable manner, or to any other person/entity specified by the customer, and includes the provision of scores, insights or analysis derived from such data to any such person.
- iv. **Account Information Service Provider (AISP)** refers to Third Party Providers (TPPs) that provides account information services.
- v. **Authentication** means a procedure used by AHIs to verify the identity of their customers.
- vi. **Bank** means a banking company as defined in section 5 of the Banking Companies Ordinance 1962.
- vii. **Consent** means an explicit indication of a customer's intention by which the customer provides agreement to the TPPs to access his/her account(s) held with an AHI for initiating payment or collecting his/her data.
- viii. **Consent Mechanism** refers to the systematic process by which AHIs and TPPs obtain, manage, and maintain explicit, informed, and revocable consent from customers for payment initiation and/or accessing, processing & sharing their financial data.
- ix. **Customer** means an individual or business entity maintaining an account(s) with AHI(s).
- x. **Customer Data** means the data in the possession of AHIs related to a customer including but not limited to account title, IBAN, account balances, payment transactions or any other transactions pertaining to current, saving, or fixed deposits or any other type of accounts.
- xi. **Encryption** is the process of converting data into a coded form to prevent unauthorized access, ensuring confidentiality and security during storage or transmission.
- xii. **Financial Institution** as defined in Payment Systems and Electronic Fund Transfers Act, 2007.
- xiii. **Multi-Factor Authentication** is a security protocol that requires customers to verify their identity using two or more independent credentials before accessing their data or initiating transactions.
- xiv. **Open Banking** refers to payments initiation and sharing of customer permissioned data with Third Party Providers (TPPs) held with AHI(s), in a standardized and secure manner to offer seamless, secure, and personalized financial products and services.
- xv. **Open Banking services** mean activities associated with the provision of payment initiation services and account information services.
- xvi. **Payment Initiation Service (PIS)** means a payment service for electronically initiating a payment order at the request of the customer for affecting the payment from his/her account or wallet held with an AHI. PIS is provided on the basis of consent provided by the customer.
- xvii. **Payment Initiation Service Provider (PISP)** means an entity that is authorized by SBP to offer payment initiation services. A PISP does not hold or maintain customer's funds at any time.
- xviii. **Regulated Entity** means a bank, MFB, EMI, PSO/PSP or TPP regulated by SBP under the applicable laws and regulations.
- xix. **Sandbox** shall refer to a live testing environment for innovative products, services, business models or technologies, pursuant to a specific testing plan, which includes some degree of regulatory lenience combined with certain safeguards.



- xx. **Third Party Provider (TPPs)** refer to AISPs and PISPs authorized by SBP under Rules for PSOs/PSPs

3) Introduction

Open Banking (OB) refers to the sharing of customer-permissioned data held by Account Holding Institutions (AHIs) with Third Party Providers (TPPs) and other financial institutions, as well as the initiation of payments from customers' accounts through authorized TPPs in a standardized and secure manner.

Broadly, OB is intended to facilitate more efficient digital payments and enable greater access to financial services in Pakistan. In particular, the regulations will facilitate business-to-business (B2B) and consumer-to-business (C2B) payments, as well as enable the use of customer data and transactional history for alternative credit assessment, thereby supporting access to finance for merchants and small and medium enterprises (SMEs).

Recognizing potential benefits and associated risks of OB, the State Bank of Pakistan (SBP) has developed these regulations with an aim to establish a robust OB ecosystem and services in the country. The regulations mandate all AHIs to provide consent-based access to customer data and payment initiation services, while adhering to highest standards of security and consumer protection.

4) Authority

These regulations are being issued by State Bank of Pakistan under powers vested through Section 3 read with Section 70 (1) of the Payment Systems & Electronic Fund Transfers Act, 2007.

5) Scope of Open Banking

The scope covers participating institutions, permissible data and accounts, services and infrastructure.

5.1 Scope of Participation

- i. All AHIs shall mandatorily expose their Application Programming Interfaces (APIs) to authorized TPPs for providing data access as defined in para 5.2, and payment initiation as per section 5.3.1.
- ii. Mandatory participation of all AHIs shall ensure that financial data of all customers (individuals and business) becomes part of the OB ecosystem from the outset.

5.2 Scope of Data and Accounts

Permissible data

- i. Account balance
- ii. Transactional history

Permissible Accounts

- i. Current Accounts
- ii. Saving Accounts
- iii. Other account (s) used for payments

5.3 Scope of Services

The licensed TPPs may offer following services under these regulations:

5.3.1 Payment Initiation Service (PIS)

Payment Initiation Services Providers (PISPs) shall offer all or any of the following:



- i. **Business-to-Business Payments (B2B)** to digitize payments of businesses across supply chain actors e.g. SMEs, retailers, distributors, and corporates.
- ii. **Consumer-to-Business Payments (C2B)** such as consumer paying to merchants for bill payments, or other products and services.
- iii. **Fund Transfer to Own Accounts** allowing businesses/merchants to transfer funds between their own accounts linked on TPP's platform.
- iv. Any other use case approved by SBP

5.3.2 Account Information Service (AIS)

By collecting data of their customers from multiple AHIs and aggregating the same, Account Information Services Providers (AISPs) shall offer the following:

- i. **Credit scoring** allows AISPs to develop credit risk profile of individuals and SMEs for onward sharing with entities regulated by SBP or SECP.
- ii. **Balance view** enables customers/SMEs to view balances of their multiple accounts at AISP's platform.
- iii. Any other use case.

5.4 Raast as Centralized API Hub

TPPs shall use the centralized API Hub of Raast for accessing customer-permissioned data held by Account Holding Institutions (AHIs), enabling them for provision of payment initiation and account information services. The AHIs and TPPs shall comply with Raast API security standards and technical integration requirements as issued by Raast Payment Pakistan (RPP).

In addition to using Raast APIs, AHIs and TPP can also enter into bilateral, or multilateral APIs arrangements through designated payment system operators for account information services, following the same security standards as have been adopted by Raast.

6) Authorization of TPP

- i. Entities intending to operate as TPPs shall obtain authorization from the State Bank of Pakistan (SBP) under the Rules for PSOs/PSPs issued in 2014.
- ii. Under authorization process, SBP shall firstly grant In-Principle Approval (IPA) to PISP and AISP. Subsequently, these entities shall approach the RPP for integration with Raast infrastructure and testing for PIS and/or AIS under sandbox.
- iii. Existing banks, EMIs, PSPs/PSOs can also offer AIS and PIS. For this purpose, these entities shall notify PSP&OD at least thirty (30) days prior to commencement of such service. Further, these entities shall be subject to the same obligations under these regulations, in respect of consent, security, conduct and liability, as applicable on the TPPs.
- iv. The TPPs shall remain subject to compliance with all applicable laws and relevant regulations, and instructions issued by SBP from time to time.
- v. In case of suspension or revocation of a TPP's authorization, RPP shall block access to TPP's requests for further access of customer data or payment initiation. Further, the concerned TPPs and AHIs shall ensure that all customer consents held by them shall stand revoked with immediate effect. Moreover, the TPP shall immediately notify all its customers, cease their access to data and payment initiation, and delete or anonymize their data in accordance with section 13 – Data Security and Privacy.



7) Consent and Authorization

AISPs and PISPs shall obtain explicit, specific and time-bound consent from their customers before providing account information and payment initiation services.

For effective consent mechanism, the following conditions shall apply:

- i. The consent shall cover scope, duration, purpose of data access and specification of payment limits along with daily and monthly limits.
- ii. Customers shall have access to a user-friendly dashboard to view, modify, or revoke active consents.
- iii. TPPs shall not request, receive, store, or use a customer's AHI login credentials, PIN, password, or any other authentication credential.
- iv. AHIs shall neither require nor permit a customer to share authentication credentials with a TPP. AHIs shall implement controls to detect and block automated access to their customer-facing channels originating from a TPP.

7.1 Consent Initiation

- i. The customer shall initiate its consent on the TPP's interface. At this stage, the TPP shall obtain the following information from the customer and display the same appropriately on the interface while providing option to the customer for any amendment or confirmation:
 - a. Name of AHI
 - b. Account information (IBAN)
 - c. Date and time of consent initiation
 - d. Consent duration
 - e. Type of data requested
 - f. Purpose of data sharing (Purpose shall be restricted as per authorized use case)
 - g. Transaction Limit (for PIS)
- ii. TPP shall initiate fresh consent whenever there is any change in the type, scope, duration or purpose of consent.

7.2 Authentication of Customers

After receiving customer's consent request, TPPs and AHIs shall authenticate customer identity to eliminate the risk of unauthorized access. For this purpose,

- i. TPP shall conduct NADRA BVS to verify customer identity and send the consent request to the AHI.
- ii. AHI shall authenticate the consent request through OTP on customer's registered mobile number.
- iii. TPP shall securely transmit AHI's OTP entered by the customer on its interface to the AHI, without storing or having visibility of the same.
- iv. After successful OTP submission by the customer, the TPP shall redirect the customer to AHI's platform for effecting authorization of consent.

7.3 Customer Authorization

- i. On AHI's platform/application, the customer shall complete authorization, using its M-PIN/T-PIN. For this purpose, the AHI shall prominently display authorization request on main screen of its platform/application to facilitate the customer in completing authorization.

- ii. After successful authorization of consent, the AHI shall immediately register the customer consent and display it on the consent dashboard on its platform/application. The consent registration shall:
 - a. Permit a TPP to access account information on behalf of the customer; or
 - b. Enable a TPP to initiate payments on behalf of the customer.
- iii. After consent registration, the AHI and TPP shall notify the customer about successful consent registration/account linking through push and in-app notifications.
- iv. AHIs shall properly retain and preserve the record the customer authorization of consent for data and payments.

7.4 Consent Management Dashboard

AHIs & TPPs shall provide their customers with an online dashboard for a real-time view of all active and past consents, allowing them to easily monitor and manage consents granted for various accounts and for multiple TPPs and AHIs.

7.5 Revocation of Consent

- i. AHIs and TPPs shall enable their customers to conveniently revoke a consent at any time through their consent management dashboard.
- ii. The entity receiving a revocation instruction shall give effect to it immediately and shall communicate it to the other entity in real-time. A revocation shall be valid and effective from the time it is received by either the AHI or the TPP, irrespective of when it is communicated to the counterparty.
- iii. Upon revocation, the TPP shall immediately cease all further access to the customer's data and shall not allow any further payment initiation. The AHI shall also decline any request made against a revoked consent.
- iv. Revocation shall not affect the validity of a payment transaction already initiated and authorized before the request for revocation.

8) Liability Architecture

Liability architecture defines how responsibilities shall be allocated among participants when any payment dispute or data breach occurs. AHIs and TPPs shall ensure that customers are protected through clear and objective liabilities rules.

8.1 Liability Provisions

- i. For PIS, an AHI shall be liable to a customer for loss or damage suffered by the customer in relation to the unauthorized payments, non-execution or late execution of a transaction, unless such loss or damage occurred as a result of any act or omission of the TPP as provided for in sub-section 8.1(iii). In such scenarios, TPP will be liable to compensate the customer.
- ii. In case of AIS, an AHI shall be liable to a customer for loss or damage suffered by the customer due to the following:
 - a. A data breach attributable to failure in the AHI's access controls, authentication mechanisms, or data governance;
 - b. Provision of inaccurate, incomplete, or outdated customer data;
 - c. Failure to cease data sharing upon receipt of a valid revocation instruction.
- iii. A TPP is liable to a customer for loss or damage suffered by the customer due to following:

- d. Unauthorized, fraudulent, or erroneous payment transactions initiated or processed through the TPP, including where such transactions result from failure to implement required authentication protocols or payment security controls;
 - e. A data breach attributable to failure in the TPP's security controls, including failure to encrypt data;
 - f. Misuse or misrepresentation of customer data, including sharing with unauthorized parties;
 - g. Failure to delete customer data upon revocation of consent.
- iv. In relation to PIS, and notwithstanding the apportionment of liability between the AHI and the TPP under this section, the AHI shall:
 - h. Upon receipt of a valid claim from the customer, credit the customer's account, within seven (7) business days of the claim is lodged.
 - i. The AHI may withhold such restoration only where it has reasonable grounds to suspect negligence on the part of the customer. AHI shall record those grounds in writing and inform the customer.
 - j. The AHI shall thereafter recover the amount from the TPP where liability is determined to rest with the TPP.
- ii. Upon identification of any unauthorized activity or data breach, the TPP/AHI shall notify the customer and SBP, as per instructions given in section 10(viii) below on Internal Control System.

8.2 Dispute Resolution Mechanism

Where a customer disputes a payment or the consent, the burden of proof shall rest with the AHI and TPP and both shall prove the following:

- i. The consent was validly obtained, authentication was correctly applied, and the transaction was accurately recorded.
- ii. The transaction was not affected by any technical or operational failure.
- iii. The mere record by an AHI or a TPP of the use of an authentication credential shall not, by itself, be sufficient to establish that the customer authorized the transaction, or that the customer acted fraudulently or with gross negligence.

Both AHI and TPP shall conduct a coordinated investigation to determine liability, with an interim status/finding provided to the customer within 7 business days. All disputes, breaches, and compensations shall be properly recorded in a centralized "Open Banking Incident Register" maintained by TPPs and AHIs.

For any disputes between AHI and TPP regarding determination of liability, Raast Payments Pakistan (RPP) shall act as Alternate Dispute Resolution forum.

9) Governance

- i. The Board of Directors of TPPs shall be responsible for setting strategic direction, approving policies, and overseeing compliance.
- ii. The TPP shall put in place an IT Steering Committee (ITSC) to oversee implementation of the TPP strategy for adoption, monitor operational effectiveness, and enforce compliance



with guidelines issued by SBP including SOPs, API security standards, and customer consent architecture.

10) Internal Control Systems

- i. TPPs shall ensure compliance with applicable data protection standards/laws issued from time to time.
- ii. TPPs shall embed security in system development, adopt secure coding practices, and harden all systems, servers, and networks.
- iii. TPPs shall establish strong internal controls for consent management, securely store records, and make them available for audits.
- iv. TPPs shall limit device and account access, and maintain a risk register for periodic risk assessments aligned with global standards.
- v. TPPs shall review incident logs, while incident response plans shall define roles, escalation paths, and communication protocols.
- vi. TPPs shall conduct periodic security testing with masked production data, and independent vulnerability assessments at least once in a year.
- vii. TPPs shall allocate adequate resources to ensure effective risk management, cybersecurity, and compliance with regulatory requirements.
- viii. TPPs shall report to SBP any incident affecting the confidentiality, integrity or availability of open banking services — including any security breach, unauthorized access, or unplanned service outage exceeding thirty (30) minutes — within two (2) hours of detection, followed by a detailed incident report within seventy-two (72) hours and a root cause analysis within fifteen (15) days.

11) Customer Recourse Mechanism

- i. TPPs shall establish and maintain a board-approved customer recourse policy in line with Business Conduct and Fair Treatment of Consumers Regulatory Framework (BC&FRF) issued by BPRD vide Circular No. 04 of 2025.
- ii. AHIs and TPPs shall implement the framework to effectively address all inquiries, complaints and disputes, raised by the customer.
- iii. The TPPs shall provide user-friendly complaint submission channels (call center, email, mobile app, etc.) and publicly disclose, in plain language, the end-to-end complaint-handling procedure.
- iv. Where a lender declines a financing request, or offers terms materially less favorable than those applied for, wholly or partly on the basis of a credit score or analysis obtained through an AISP, the lender shall inform the customer of that fact, identify the AISP, and advise the customer of the right to obtain the underlying information.
- v. TPPs shall inform customers of a formal dispute resolution mechanism to be followed in cases where the customer is not satisfied with initial outcome of his/her complaint.
- vi. AHIs & TPPs shall comply with the timelines for complaints/disputes resolution, as given under SBP regulatory instructions issued from time to time.
- vii. AHIs & TPPs shall conduct customer awareness programs for their customers so that they understand their rights, and the available recourse options.
- viii. The details of complaint lodgment and disputes escalation are placed at **Annexure-A**

12) AML/CFT/CPF Requirements

- i. TPPs shall implement necessary KYC/CDD controls for consumers and merchants.
- ii. While onboarding merchants/businesses, TPPs shall comply with the requirements as given in the customer onboarding framework issued by BPRD vide circular 01 of 2025. For



this purpose, TPPs shall obtain minimum set of verified documents for KYC purpose as stipulated in **Annexure-B**.

- iii. Whenever there is change in the business profile of merchant/SME/corporate or any business entity, TPPs shall update the risk profile and may also communicate the same to AHI for risk profile updation at their end.
- iv. Where a TPP, in the course of providing open banking services, forms a suspicion that a transaction or a customer/merchant account activity may be related to money laundering, terrorist financing or proliferation financing, it shall report the suspicion to the concerned AHI without delay.

12.1. Mitigation of ML/TF/PF Risk

AHIs shall continue to bear the primary responsibility of ML/TF/PF risk mitigation of consumers and merchants.

- i. Further, AHIs and TPPs shall:
 - a. Adopt risk-based approach for ML/TF/PF Risk mitigation for AIS and PIS
 - b. Identify ML/TF/PF threats & vulnerabilities in TPP services and update the profile of the customer where required.
 - c. AHI shall monitor the payments initiation and report any suspicious transaction as per the existing AML/CFT/CPF regulations.
 - d. TPP shall keep record of each payment initiated by customer and ensure it is purpose specific (B2B or C2B).

13) Data Protection, Security and Privacy

- i. AHIs and TPPs shall uphold the highest standards of data security and privacy in line with BPRD Circular No. 5 of 2017, BPRD Circular No. 4 of 2023 and PSP&OD Circular No. 4 of 2025, ensuring data protection throughout its lifecycle with access restricted to entities authorized under these regulations, and limited to the data and the purposes for which the customer has given consent.
- ii. Upon revocation or expiry of a consent, the TPP shall within thirty (30) days delete or irreversibly anonymize all customer data and any other results generated through processing of such data, obtained under that consent and shall confirm the same to the customer. This obligation shall not extend to:
 - a. Consent records and audit logs required under relevant laws and regulations
 - b. Records required for a pending complaint, dispute, investigation or legal proceeding.
 - c. Data retained under the proviso 13(ii) (b) shall be held in a segregated, access-restricted environment, shall be used solely for the purpose for which it is retained, and shall not be used for any commercial or analytical purpose.
- iii. Customer data obtained under these regulations shall be stored and processed within Pakistan, unless such data is stored or processed through a cloud service provider in accordance with the Framework on Outsourcing to Cloud Service Providers issued vide BPRD Circular No. 01 of 2023, as amended from time to time.
- iv. A TPP shall ensure that any score, insight or analysis derived from customer data is limited to what is relevant to the purpose consented to, and shall not derive or disclose inferences about a customer's personal affairs that are not relevant to that purpose.
- v. Every director, officer, employee, agent and contractor of a TPP having access to customer data obtained under these regulations shall, before assuming such access, furnish a written declaration of fidelity and secrecy in the form prescribed by the TPP's board-approved policy, and shall remain bound by it after the relationship ends.



- vi. These measures shall guarantee secure and transparent handling of customer data across all TPP operations.

14) UI/UX Guidelines

- i. TPPs and AHIs shall design user-friendly customer journeys by showing key payment details upfront, providing instant confirmations, enabling cancellation or modification before fund transfer, offering retry/help options, displaying clear security icons, ensuring transparent redirection for authorization, and minimizing extra steps.
- ii. TPPs and AHIs shall avoid practices that create frictions, including excessive text or scrolling, confusing wording, repeated requests, toggling between screens, reentering already authenticated information, discouraging messages about licensed TPPs, or displaying ads and product cross-selling.

15) Pricing of product and services

To promote digital payments and adoption across ecosystem, RPP shall not charge TPPs for payments initiation and data sharing. In line with these objectives, the pricing arrangement between AHIs and TPPs shall also be kept reasonable, and shall be mutually agreed between TPPs and the representative body of AHIs.

TPPs shall adhere to the following principles for pricing their products and services for customers:

- i. TPPs offering C2B payments shall not charge the customers initiating payments.
- ii. Similarly, TPPs shall keep the pricing level for the corporate, retailers, SMEs merchants below the existing price level prevailing in market to promote adoption of digital payments for merchants and businesses.
- iii. The pricing shall be easy to understand, and clearly communicated to merchants and businesses.
- iv. TPPs shall take into account scale of services and usage pattern of their consumers.
- v. All pricing details shall be clearly provided on the TPP website/application.
- vi. TPPs shall decide which services shall be free of cost to encourage wider adoption.
- vii. TPP shall align their pricing model with SBP's framework for consumer protection and fair treatment of customers.

16) Compliance with Existing Regulatory Frameworks

For the purpose of open banking, AHIs shall continue to comply with all applicable laws, regulations, and instructions issued by SBP, including but not limited to:

- i. Enterprise Technology Governance & Risk Management Framework for Financial Institutions, issued vide BPRD Circular No. 05 of 2017, as amended from time to time.
- ii. Framework for Risk Management in Outsourcing Arrangements by Financial Institutions issued vide BPRD Circular No. 06 of 2019, as amended from time to time, for governance and risk management of outsourcing activities.
- iii. Instructions on Fair Treatment of Consumers, including Business Conduct and Fair Treatment of Consumers Regulatory Framework (BC&FRF) issued vide BPRD Circular No. 04 of 2025, for customer recourse, complaint handling, and consumer protection.
- iv. Measures to Enhance Security of Digital Banking Products and Services issued vide BPRD Circular No. 4 of 2023.



- v. Mobile Applications (Apps) Security Guidelines Issued vide PSP&OD Circular No. 01 of 2022.
- vi. All relevant Anti-Money Laundering, Countering the Financing of Terrorism, and Countering Proliferation Financing (AML/CFT/CPF) regulations and directives applicable to financial institutions.

TPPs authorized under the Rules for Payment System Operators/Payment Service Providers (PSOs/PSPs), shall continue to comply with all applicable laws, regulations, and instructions issued by SBP, including but not limited to:

- i. Rules for PSOs/PSPs, issued vide PSD Circular No. 03 of 2014 (as amended), and any subsequent instructions governing their licensing, capital, and operational conduct.
- ii. Technology Risk Management Framework for Payment Institutions, for all matters pertaining to governance and oversight, technology and cyber risk management, digital fraud management, outsourcing, disaster recovery, business continuity, and security testing (including vulnerability assessments and penetration testing).
- iii. Instructions on Fair Treatment of Consumers, including Business Conduct and Fair Treatment of Consumers Regulatory Framework (BC&FRF) issued vide BPRD Circular No. 04 of 2025, for customer recourse, complaint handling, and consumer protection.
- iv. Mobile Applications (Apps) Security Guidelines Issued vide PSP&OD Circular No. 01 of 2022.
- v. All relevant Anti-Money Laundering, Countering the Financing of Terrorism, and Countering Proliferation Financing (AML/CFT/CPF) regulations and directives applicable to payment service providers.

Annexure-A – Rules for Customer Recourse Management**1) Customer Complaint Mechanism**

<u>Rule No.</u>	<u>Rule</u>	<u>Explanation</u>
1	Multi-Channel Intake	TPPs and AHI shall provide a variety of channels—email, phone, in-app chat, web form, and in-branch—to suit customer's preferences.
2	24/7 Complaint Acknowledgment	Every complaint shall be auto-acknowledged within one hour of the receipt and shall send a personalized reply within 24 hours.
3	Unique Tracking ID	AHI and TPP shall provide a unique reference number upon complain lodgment by customer. Customers should be able to check status online or via SMS.
4	Tiered Escalation	AHI and TPPs shall ensure that complaints flow up the defined hierarchy. Each level shall have explicit responsibilities & deadlines.
5	Turn Around Time	TPPs and AHIs shall follow the guidelines for TATs as per the regulatory instructions issued by SBP.
6	Transparent Communication	AHIs and TPPs shall update customers at every step including receipt, investigation and resolution.
7	Data Privacy & Security	All complaint records shall reside in an encrypted and access-controlled system.
8	Standardized Categorization	Complaints shall be tagged by type e.g. unauthorized transaction, service quality, technical glitch, etc.
9	Customer Feedback Loop	After closure of complaint, AHI and TPP shall send a satisfaction survey with open ended feedback form.

2) Dispute Resolution Mechanism

<u>Rule No.</u>	<u>Rule</u>	<u>Explanation</u>
1	Clear Eligibility Criteria	TPP and AHI shall devise a policy to explicitly define which scenarios qualify as disputes (fraud, billing errors, data breach, etc.).
2	Formal Submission Format	AHI and TPP shall ensure that documentation of dispute consists of a concise written statement, relevant dates, amounts, and supporting documents.
3	Independent Case Manager	AHI and TPP shall hand over the case to an independent unit (, one not involved in complaint handling).
4	Evidence Collection Protocol	TPP and AHI shall secure system logs, call recordings, transaction audits, and customer documentation.



5	Structured Investigation	TPP and AHI shall conclude initial findings within 7 working days and share the same with the customer. TPP and AHI shall ensure that the dispute is resolved within the timeline of 30 days.
6	Alternative Dispute Resolution	TPP and AHI shall guide if the customer wants to escalate the dispute to SBP.

3) Customer Compensation and Closure

<u>Rule No.</u>	<u>Rule</u>	<u>Explanation</u>
1	Immediate Action	TPP and AHI shall ensure that immediate action is taken, once the assessment or outcome of the complaint is found in favor of the customer.
2	Reimbursement	TPP and AHI shall ensure that the customer is compensated immediately as mentioned in section 8 of these regulations
3	Customer Satisfaction Letter / Acknowledgement	For each complaint that is settled in favor of the customer, it shall be backed by a customer satisfaction letter or digital acknowledgement.

Annexure-B -Minimum Set of Documents required for Onboarding/Sign-up by TPPs

KYC Requirement	For Individuals	For Business Entities
1. Information to Collect		
Identity	Full Name, Date of Birth	Business Name
Address/Contact	Residential Address, Verified Email & Mobile Number.	Business Address
Business Details	Not Applicable.	Nature of Business, Business Registration Number
Ownership & Control	Not Applicable.	Name of owners/shareholders
2. Verification & Documentation		
KYC Requirement	For Individuals	For Business Entities
Identity Verification	CNIC/passport and its expiry	CNICs of all Directors
Business documentation	Not Applicable.	a. Self-declaration for sole proprietor b. Incorporation certificate for registered businesses

Requirements for TPPs for onboarding/acquiring of merchants/businesses**1. KYC of merchants for collections.**

Before enabling payment collections for merchants through PIS, the TPP shall:

- Verify the merchant's identity and beneficial ownership.
- Obtain and assess the nature and location of the business, relevant websites/applications, constituent documents and FBR registration, as applicable.



- c. Verify that the bank account/wallet provided by the merchant is maintained in the merchant's name. For the purpose, PISP may contact the relevant merchant's account servicing institution for verification.
- d. Obtain and verify utility bills
- e. Obtain expected transaction volumes and values, assign a documented merchant risk rating and conduct additional verification of business activities and supporting documents for higher-risk merchants.

2. Monitoring

The TPPs shall:

- a. Require merchants to notify changes in ownership/control, business activities, websites/applications or receiving accounts.
- b. Obtain and update the information of major suppliers and customers.
