**📌 Cards and Payments – Types, Workflow, and Examples**

**1️⃣ What is a Payment System?**

A **payment system** is a network that enables financial transactions between parties. It includes methods like **credit cards, debit cards, digital wallets, UPI, wire transfers, and BNPL (Buy Now, Pay Later)**. These payments involve multiple entities such as **merchants, banks, payment processors, and regulatory bodies**.

**2️⃣ Types of Payment Cards & Their Workflows**

**🔹 1. Credit Cards**

A credit card **allows users to borrow money** from the issuing bank up to a pre-approved credit limit for purchases.

**💳 Workflow (Example: Amazon Purchase using a Credit Card)**

1️⃣ The customer enters credit card details (16-digit PAN, CVV, expiry).  
2️⃣ Merchant sends the transaction request to the **Acquirer Bank**.  
3️⃣ The Acquirer forwards the request to the **Card Network (Visa/Mastercard)**.  
4️⃣ The **Issuer Bank** (bank that issued the card) checks:

* Credit limit
* Fraud detection
* CVV validation  
  5️⃣ The Issuer **approves or declines** the transaction.  
  6️⃣ If approved, the money is **debited later** from the customer's bank after the billing cycle.  
  7️⃣ The **Merchant gets paid** by the Acquirer.

✅ **Example:** Using an **HDFC Credit Card** to buy a laptop on Amazon.

**🔹 2. Debit Cards**

A debit card **directly deducts funds** from the customer’s bank account instead of borrowing credit.

**💳 Workflow (Example: Swiping a Debit Card at a POS Machine)**

1️⃣ The customer swipes/dips the debit card at a **POS terminal**.  
2️⃣ The POS machine sends a request to the **Acquirer Bank**.  
3️⃣ The Acquirer forwards the request to the **Card Network** (Visa/Mastercard/RuPay).  
4️⃣ The **Issuer Bank** checks:

* Sufficient balance
* CVV verification
* Fraud detection  
  5️⃣ If the transaction is **approved**, the amount is **instantly deducted** from the customer’s account.  
  6️⃣ The **Merchant receives the money** from the Acquirer Bank.

✅ **Example:** Using an **ICICI Debit Card** to pay at McDonald's via a POS machine.

**🔹 3. Prepaid Cards**

A prepaid card is **preloaded with a specific balance** and can be used until the balance runs out.

**💳 Workflow (Example: Using a Prepaid Gift Card for Online Shopping)**

1️⃣ Customer enters a prepaid card number on an **e-commerce site**.  
2️⃣ The payment request goes to the **Card Network (Visa/Mastercard/RuPay)**.  
3️⃣ The Issuer checks:

* Available balance
* Card expiry  
  4️⃣ If the balance is sufficient, the payment is **approved**, and the amount is deducted.  
  5️⃣ The **Merchant gets paid** by the Acquirer.

✅ **Example:** Using a **Flipkart Gift Card (Prepaid)** for an online order.

**🔹 4. Virtual Cards**

Virtual cards are **temporary, disposable card numbers** linked to a credit or debit account for secure online transactions.

**💳 Workflow (Example: Booking a Flight Using a Virtual Card)**

1️⃣ A virtual card is **generated via the bank’s mobile app** (e.g., HDFC NetBanking).  
2️⃣ The customer enters the **virtual card number** on a travel website.  
3️⃣ The **payment request is processed** via the Card Network.  
4️⃣ The Issuer Bank **approves** the transaction.  
5️⃣ The virtual card **expires** after one-time use or a fixed period.

✅ **Example:** Using an **Axis Bank Virtual Card** for a **MakeMyTrip** booking.

**🔹 5. Contactless Payments (Tap & Pay / NFC Cards)**

Near Field Communication (NFC)-enabled cards allow payments by **tapping the card** on a reader without entering a PIN for small transactions.

**💳 Workflow (Example: Paying for Metro Fare Using a Contactless Card)**

1️⃣ Customer **taps** the card on the NFC-enabled **Metro gate**.  
2️⃣ The card details are sent to the **Card Network**.  
3️⃣ The Issuer Bank checks:

* Contactless limit (e.g., ₹5000 in India)
* Fraud risk  
  4️⃣ If approved, the amount is **instantly debited**, and the gate opens.

✅ **Example:** Using an **SBI Contactless Debit Card** to pay at a Metro Station.

**3️⃣ Payment Systems & Their Workflows**

**🔹 1. UPI (Unified Payments Interface) – Real-Time Bank Transfers**

UPI allows **instant money transfer** between bank accounts using a UPI ID or QR code.

**💳 Workflow (Example: Paying via Google Pay at a Restaurant)**

1️⃣ Customer scans the **merchant’s QR code**.  
2️⃣ The request goes to the **NPCI (National Payments Corporation of India)**.  
3️⃣ NPCI forwards the request to the **Payer’s Bank (e.g., SBI)**.  
4️⃣ The Payer’s Bank verifies:

* UPI PIN
* Sufficient balance  
  5️⃣ If approved, the money is instantly transferred to the **Merchant’s Bank Account**.

✅ **Example:** Paying at **Domino’s Pizza** using **Google Pay (UPI)**.

**🔹 2. Wallet Payments (Paytm, PhonePe, PayPal, Apple Pay, Google Pay)**

E-Wallets store **preloaded money** or link to a credit/debit card for online/offline payments.

**💳 Workflow (Example: Paying with Paytm at a Supermarket)**

1️⃣ Customer **opens Paytm** and scans the QR code.  
2️⃣ Paytm **deducts balance** from the linked bank account or wallet.  
3️⃣ The amount is instantly transferred to the **Merchant’s Paytm account**.

✅ **Example:** Using **Paytm Wallet** at **Reliance Fresh**.

**🔹 3. BNPL (Buy Now, Pay Later) – Deferred Payments**

BNPL services like **ZestMoney, Simpl, LazyPay** allow users to **purchase now and pay later** in installments.

**💳 Workflow (Example: Using LazyPay for Online Shopping)**

1️⃣ Customer selects **LazyPay** as the payment method on an e-commerce site.  
2️⃣ LazyPay verifies **credit limit & user identity**.  
3️⃣ If approved, LazyPay **pays the Merchant instantly**.  
4️⃣ The customer repays **LazyPay in EMIs** after a few weeks.

✅ **Example:** Buying a smartphone on **Flipkart using ZestMoney**.

**🔹 4. IMPS (Immediate Payment Service) – Instant Bank Transfers**

IMPS is used for **instant bank-to-bank money transfers** via mobile banking apps or net banking.

**💳 Workflow (Example: Sending Money via SBI NetBanking IMPS)**

1️⃣ The user enters the **beneficiary’s account details & IFSC**.  
2️⃣ The **Payer’s Bank (SBI)** sends a request to **NPCI**.  
3️⃣ NPCI forwards the request to the **Beneficiary’s Bank (HDFC)**.  
4️⃣ If all validations pass, funds are **instantly transferred**.

✅ **Example:** Sending ₹10,000 from **SBI to HDFC via IMPS**.

**📌 Conclusion**

Payments can be done via **Cards (Credit/Debit/Prepaid), UPI, BNPL, Wallets, and IMPS**. Each method has **different workflows, security mechanisms, and validation processes**.

**📌 Key Compliance Standards in Payments for QA Testers**

As a **QA tester in the banking/payments domain**, understanding **PCI DSS, EMV, and PSD2** is crucial for ensuring secure, compliant, and high-quality payment systems. Below is a **detailed breakdown** of each compliance standard and what **QA testers should know** while testing payment applications.

**🔹 1. PCI DSS (Payment Card Industry Data Security Standard)**

**PCI DSS** is a **global security standard** designed to **protect cardholder data** and ensure **secure payment processing**. It applies to businesses handling **credit, debit, and prepaid card transactions**.

**📌 Key PCI DSS Requirements for QA Testing**

1️⃣ **Data Encryption:**

* Ensure **card numbers (PAN), CVV, and sensitive data** are **encrypted** before storage or transmission.
* Test whether **TLS 1.2+ encryption** is used for secure communication.

2️⃣ **Masking of Cardholder Data:**

* PAN should be **masked** (e.g., XXXX-XXXX-XXXX-1234) in logs, UI, and receipts.
* Full card numbers should **never be displayed** or stored in plaintext.

3️⃣ **Authentication & Access Control:**

* Only **authorized personnel** should access sensitive cardholder data.
* **Multi-Factor Authentication (MFA)** should be enabled for admin users.

4️⃣ **Secure Transmission of Data:**

* Ensure **HTTPS** is used for online transactions.
* Validate that **end-to-end encryption (E2EE) or tokenization** is implemented.

5️⃣ **Vulnerability Scanning & Penetration Testing:**

* Regular **security testing** should be conducted on the system.
* Ensure **firewall & intrusion detection systems (IDS/IPS)** are in place.

**📌 Key QA Testing Scenarios for PCI DSS Compliance**

✅ Test that **card details are never stored** in plaintext.  
✅ Verify that **logs do not contain sensitive data** like CVV.  
✅ Ensure that **expired sessions log out users automatically**.  
✅ Perform **penetration testing** to check for vulnerabilities.

**🔹 2. EMV (Europay, Mastercard, Visa) Standard**

**EMV** is a security standard for **chip-based credit & debit card transactions**, reducing fraud compared to traditional **magnetic stripe** cards.

**📌 Key Features of EMV for QA Testing**

1️⃣ **Chip-Based Transactions:**

* Ensure transactions are authenticated using **EMV chip** and **PIN/signature**.

2️⃣ **Card Authentication & Processing:**

* Validate if the system **correctly differentiates** between **Chip & PIN**, **Chip & Signature**, and **Contactless (NFC)** transactions.

3️⃣ **Tokenization:**

* EMV cards use **dynamic cryptograms** instead of static data to prevent fraud.
* QA should ensure that every transaction generates a **new token**.

4️⃣ **Fallback Handling:**

* If a chip reader fails, the system should allow a **magnetic stripe fallback**, but only after security checks.

**📌 Key QA Testing Scenarios for EMV Compliance**

✅ Test **chip-based transactions** using real EMV cards.  
✅ Verify **contactless payments (Tap & Pay)** on POS terminals.  
✅ Ensure proper **handling of card declines** due to authentication failures.  
✅ Test **fraud prevention mechanisms** (e.g., failed PIN attempts leading to card blocking).

**🔹 3. PSD2 (Revised Payment Services Directive – Europe)**

**PSD2** is a **European regulation** that enhances security in **online banking & digital payments**, promoting **Open Banking**.

**📌 Key PSD2 Requirements for QA Testing**

1️⃣ **Strong Customer Authentication (SCA):**

* Online payments require **Multi-Factor Authentication (MFA)**:  
  ✅ Something the user **knows** (password, PIN)  
  ✅ Something the user **has** (OTP, mobile app)  
  ✅ Something the user **is** (biometrics – fingerprint, facial recognition)

2️⃣ **Open Banking & API Security:**

* Banks must provide **secure APIs** for **third-party payment services (TPPs)**.
* QA must test API security, **OAuth 2.0 authentication**, and **token expiration**.

3️⃣ **Transaction Monitoring & Fraud Prevention:**

* Transactions must be **monitored in real-time** for fraud detection.
* QA should verify **risk-based authentication (RBA)** mechanisms.

**📌 Key QA Testing Scenarios for PSD2 Compliance**

✅ Verify **MFA login flows** (OTP, biometrics).  
✅ Ensure **secure API authentication** with third-party providers.  
✅ Test **failed authentication scenarios** (wrong OTP, expired token).  
✅ Check **fraud alerts** for unusual transactions.

**🔹 Summary: QA Checklist for PCI DSS, EMV, and PSD2**

| **Standard** | **Key Focus** | **QA Test Cases** |
| --- | --- | --- |
| **PCI DSS** | Secure storage & transmission of card data | ✅ Test **encryption** & **masking** of PAN/CVV ✅ Check **access control** & **logging** rules |
| **EMV** | Chip-based transactions & fraud prevention | ✅ Test **chip & PIN/signature** transactions ✅ Verify **tokenization** for secure payments |
| **PSD2** | Open banking, MFA & fraud detection | ✅ Test **MFA for online payments** ✅ Verify **secure API authentication & fraud alerts** |

**📌 Final Thoughts**

As a **QA tester in banking/payments**, you must ensure that payment applications comply with **PCI DSS, EMV, and PSD2 regulations** to protect cardholder data and prevent fraud.