BARCLAYS BANK

DIGITAL PAYMENT PRODUCTS & SERVICES SECURITY POLICY

DOCUMENT DETAILS

Policy Title	Digital Payment Product and Services Policy
Date Approved	
Approving Body	India ExCo
Implementation Date	
Related Directions & Regulations	RBI - Master Direction on Digital Payment Security Controls
Related Policies	Information Refer appendix for all the related policies.
Version	3.1
Frequency of Review	Annual
Policy Owner Department	Bindu Seth | Head Cash Products & Geeta Sahdev | Head Branch
Policy User Departments	All Departments

Contents

1. Summary of Changes from Last Version

Date	Version	Description	Changed By	Details of Change
21/07/2021	1.0	Original	N A	Policy Created
31/10/2023	2.0	Review of Policy	Sandy Miranda	NA
31/01/2024	3.0	Review of Policy	Sandy Miranda	NA
25/04/2024	3.1	Amendment to section on Fraud Risk Management	Paresh Tamhankar	Amendment to the section on Fraud Risk Management 5.5 & 5.6
25/04/2024	3.1	Addition of 'external assessment' annually	Sandy Miranda	Sec 4.6 of the document.

1.1 Document Change Control

Sr.No.	Name	Organization	Purpose
1	Ms. Bindu Seth	Barclays Bank	Review & Approve
2	Mr. Deepak Sah	Barclays Bank	Review & Approve
3	Mr. Subramanian K G	Barclays Bank	Review & Approve
4	Mr. Harshad Dalvi	Barclays Bank	Review & Approve
5	Mr. Paresh Tamhankar	Barclays Bank	Review & Approve
6	Mr. Yogesh Mahadkar	Barclays Bank	Review & Approve
7	Ms. Paola Montilla	Barclays BI CISO	Review & Approve
8	Mr. Santosh Bhagwat	Barclays Bank	Review & Approve

2. Purpose and Contextual Information

The digital payments ecosystem has seen rapid growth with a strong movement towards a cashless economy. It thus becomes important to understand the challenges that come along with it. One of the biggest challenges and most important aspects when it comes to digital payments is security. In the present technology enabled world, strengthening cybersecurity is imperative, to build a secure digital payments ecosystem. This policy is in line to build a secure environment during Digital payment transactions and to set up a robust structure for such systems and implement common minimum standards of security controls for channels like the internet banking, mobile banking, card payments, among others. While the guidelines will be technology and platform agnostic, they will create an enhanced and enabling environment for customers to use digital payment products more safely and securely.

2.1 Policy Statement

All sites, applications, and products, which relate to Digital payments and house the Bank's critical information as well as customer data, shall provide resistance to unauthorized access and protection against cyber threats. Access to these websites/applications shall be logged, monitored, and reviewed.

It is the purpose of the policy to ensure that:

a) Adequate controls to protect the **confidentiality of customer data and integrity of data** and processes associated with the digital payment product/ services offered.
b) Availability of stipulated infrastructure e.g. People, Process, Technology etc. with necessary backup.
c) Assurance of payment product's **robust performance** ensuring security, consistency and rolled out after necessary testing for achieving desired Functionality, Security & Performance specifications.
d) Capacity strengthening and expansion with **scalability.**
e) Minimal customer service disruption with **high availability** of systems/ channels.
f) Methodical and effective **dispute resolution mechanism** and handling of **customer grievance**, and
g) Adequate **review mechanism** along with swift corrective action, if any one of the mentioned requirements is getting hampered or having high potential to get hampered.

2.2 Tolerance Statements

Barclays has zero tolerance for:

1. Control gaps rated as critical (for which we have no remediation activities in place)
2. Employees/contractors deliberately bypassing security controls for personal gain or to harm the bank.
3. Cyber Attacks resulting in: Unavailability of systems beyond set Recovery Time or Recovery Point Objectives (where defined)

3. Scope and Adherence

3.1 Scope

Unless otherwise stated in the Group Policy, the following scope clauses apply:

In Scope

This Policy applies to:

- Barclays Bank PLC (India Branch)
- All Information assets involving customer enabling digital payment channels and its data hosted in Bank's website, applications, network, security devices, servers and other IT system that needs to be appropriately protected from unauthorized access as well as cyber threats.
- All employees of Bank including all IT personnel viz. (system, database, application, network administrators) and Physical security personnel are responsible for securing and monitoring such digital payment related data in the Bank premises.
- All Third-Party personnel (related to digital payment processes) who work within the Bank premises.

3.2 Adherence

The provisions of this Policy are mandatory and are used to direct the controls required for managing the Governance, Risk and Control Processes around Digital Payment Systems. Any deviations must be escalated to the Policy and/or Standard Owner in line with the Barclays Control Framework and associated documents.

3.3 Compliance with Applicable Laws, Rules, Regulations and Supervisory Requirements

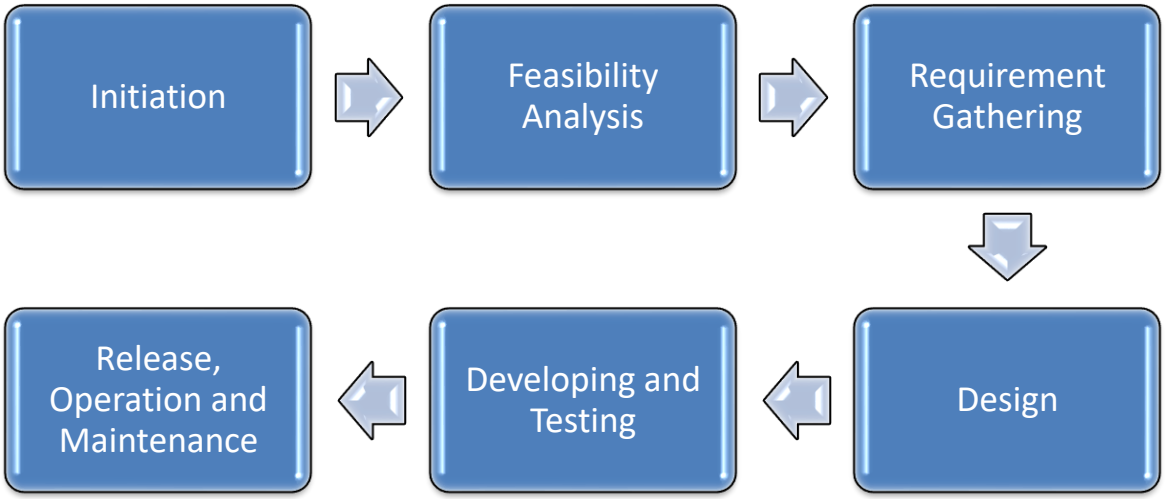
Any identified contravention of or non-conformance with laws, rules, regulations or associated supervisory requirements applicable to this Policy must be escalated in accordance with the Barclays Control Framework and recorded in the applicable Risk and Control management system(s).

3.4 Reputational Impact

Any action taken or inaction relevant to this document which may have potential to incur Reputation Risk for Barclays, i.e. likely to result in material criticism and / or censure of Barclays by key stakeholders or opinion formers (including customers, clients, market counterparties, regulators, legislators, media or Non- Governmental Organizations (NGOs)), must be identified, evaluated, reported and escalated in accordance with the Barclays Reputation Risk Management Framework.

4. Introducing a digital payment product

This section specifies the design, development, commissioning, procurement, up-gradation and operation of the Digital Payment system and its data in such a way that information security and application security risks are assessed, understood and addressed by implementing appropriate process and technology controls.



The following phases shall be followed during the introduction or inception of a digital payment product:

4.1 Initiation phase

- All new initiatives, products, services, business activities in scope of the **New and Amended Product and Service Approval** (NAPA) Standard must go through NAPA governance.
- The Business must ensure that they have appropriate governance in place to identify and manage all in scope product design proposals prior to entering the NAPA process. Where there is any uncertainty regarding scope, the BU NAPA team must be consulted to determine if in/ out of scope.
- Requirements related to information security shall be included in every new information system, current information systems evolution or service provision. Identification of these requirements must rely on the processes implemented. These requirements must be validated by the Global CSO team. Any security requirement in the application should be based on the threat model. The bank shall develop, define, document, adopt and incorporate a threat modelling approach during application lifecycle management. The approach shall identify security requirements, pinpoint security threats and potential vulnerabilities, quantify threat and vulnerability criticality, and prioritize remediation methods.
- Information to be processed by the new software shall be classified according to the Bank's "Group Information and Cyber Security policy".

- The development team / System Engineers/ Architects shall follow bank's "Technology Application Development Standard" to ensure to include representatives from the information security and/or application security team to ensure the adequate information security controls are considered during all phases of the system life cycle.
- An adequate Backup and Disaster Recovery plan shall also be finalized before an application is migrated into production.
- Provide secure coding awareness training to the developers at least annually once.
- The network team shall analyze the impact on existing systems before adding any new network connections. Security vulnerabilities must be considered while designing connectivity or interface with other systems and applications.
- For digital payment applications that are licensed by a third-party vendor, Bank staff shall have an escrow arrangement for the source code to ensure service continuity in case the vendor is unable to provide services or discontinues maintenance and support of the software.

4.2 Feasibility Analysis

- The designated application security team shall perform an application risk analysis to determine the security controls required for the system or system application under development. The risk analysis should be based on but not limited to the requirements from compliance, fraudulent related risks, vulnerabilities, and threats.
- The application security team would review all the requirements and provide security-related requirements before the start of the design phase.
- The team shall seek a high-level understanding of the system that needs to be developed. Based on the information collected during the initiation phase a comprehensive project plan is prepared with contains the following aspects.

    - Key phases of the project and goals to be achieved,
    - Target dates for completion and reaching the goals,
    - Resources required for completing various phases of the project,
    - Documentation required during the project, and
    - Formation of the entire project team.

4.3 Requirement phase

Information systems security requirements shall be explicitly defined (including protection of customer information/ data) during (a) requirements gathering, (b) designing, (c) development, (d) testing including source code review, (e) implementation, maintenance & monitoring and (f) decommissioning phases of the digital payment applications:

- Be based on the output from a risk assessment to be performed as a part of the Initiation phase/Feasibility phase.
- Reflect the business value of the information assets involved and the potential impact of a compromise in confidentiality, integrity, and availability of these information assets.
- Product-level limits on the level of acceptable security risk, document specific security objectives and performance criteria including quantitative benchmarks for evaluating the success of the security built into the digital payment product shall be documented.

- The actual results with projections and qualitative benchmarks shall be periodically reviewed to detect and address adverse trends or concerns. Automated security controls (egg: web application firewall) to be incorporated in the systems along with supporting manual controls designed to reduce the risks of security compromise if need be
- Comply with relevant legal, contractual and any other requirements, if any.
- Once the security requirements have been defined, modifications to the system's proposed configuration, functionality and information assets shall be accompanied by a review and re-definition, as necessary, of the security requirements. The relevant application security team would assess and confirm the requirements specification process and if meets the required security standards defined within Barclays Bank.

4.4 Design phase

- Security specifications for the new software shall be documented to provide the development group with specific requirements. This enables Barclays Bank in identifying, reviewing and testing the security functionalities of the software.
- System and physical architecture, interfaces, manual processes and documentation with respect to design phase shall be documented. Every digital payment products/ services offered should record the mechanics, clear definition of starting point, critical intermittent stages/ points and end point in the digital payment cycle, security aspects, validations till the digital payment is settled, in a documented form. Clear pictorial representation of digital path and exception handling should be captured in documented form.
- The bank shall ensure that wherever HSM, ATM and other card related processes are outsourced to third party service provider, appropriate security measures and standard payment cards standards (PCI - DSS), and standards such as PCI-PIN for secure management processing and transmission of PIN, PCI-PTS including security approval framework that addresses the logical and physical protection of the cardholder, PCI-HSM for securing cardholder-authentication applications and processes including key generation, PIN verification etc shall be contractually enforced on the said third party for compliance. For further reference please refer to Third Party Service Provider Management Standard and External Supplier Control Obligations
- The system and physical architecture, interface and manual process shall be tested against security best practices. The following elements should be considered in the design phase to mitigate risk. These include:
    - Identifying threats and defining a mitigating plan. The threat analysis can be carried out throughout the system development life cycle. In each phase threat and its mitigation elements are detected
    - Perform security risk assessment
    - Develop a plan to migrate current data to the new system
    - Defining the operating environment, at the end of this phase, a software architecture document should be created.

4.5 Developing and testing phase

- This Development phase integrates all the components of the System or Application based on the design. During development, the following steps occur.
- The executable code is created. Source code review is performed after the integration phase, to identify the design level flaws
- The required files and databases are built and populated.
- The hardware, software and communications necessary to support the development effort are assembled and reviewed against security best practices.
- The documents to support testing, implementation and maintenance of the system shall be compiled.
- The application developer team's manager shall perform an independent review of the test results and shall formally sign off on the test results.
- Wherever third-party service providers are engaged, adequate oversight and controls for monitoring the activities of the third-party personnel shall be documented in and assessed based on "Third Party Service Provider Management Standard" and their respective "External Supplier Control Obligations (SCO)" as established by the bank.
- All modifications, enhancements and installation or implementation of new systems shall be subject to "Integration Test" and "User Acceptance Test" by the appropriate teams before installation into production. Appropriate quality assurance team with the application security team shall review the changes/new products before moving to live.
- Infrastructure security assessments and application security assessments should be performed. Bank's IT department / Penetration Testing department shall conduct security testing including review of source code, Vulnerability Assessment and Penetration Testing (VAPT) of their digital payment applications to assure that the application is secure for online transactions while preserving confidentiality and integrity of the data that is stored and transmitted. Such testing should be compliant with various standards like (OWASP). If the source code is not owned by the Bank then IT personnel shall obtain a certificate from the application developer, which states that the application is free of known vulnerabilities, malware, or any covert channels in the code. In this context:
    - The Vulnerability Assessment shall be conducted at least on a half-yearly basis while the Penetration Testing shall be conducted at least every year. In addition, VA/PT shall be conducted as and when any new IT Infrastructure or digital payment application, services or product are introduced or when any major change is performed in the application or infrastructure.
    - Testing or Certification should broadly address the objective that the application's version and module(s) functions only in a manner that it serves the intended purpose, is developed as per the best secure design, coding practices and standards, and addresses new threats due to insecure coding.
    - Testing that reviews source code or certification shall be conducted/ obtained. This shall continue every year if any changes or upgrades have been made to the application during the year.
    - Penal provisions shall be included by the Bank into third-party contractual arrangements for any non-compliance by the application provider.

- Barclays shall compare the results from earlier vulnerability scans to verify/ ascertain that vulnerabilities are addressed either by patching, implementing a compensating control, or documenting and accepting the residual risk with necessary approval and that there is no recurrence of the known vulnerabilities. The identified vulnerabilities should be fixed in a time-bound manner.

- Barclays shall ensure that all vulnerability scanning is performed in authenticated mode either with agents running locally on the system to analyse the security configuration or with remote scanners that are given administrative rights on the system being tested.

- Barclays shall verify and thoroughly test the functionality (to validate whether the system meets the functional requirements/ specifications) and security controls of payment products and services before its launch/ moving to the production environment.

- OWASP Application Security Verification Standard (ASVS), application security requirements shall be referenced for guidelines to ensure the development, rollout and maintenance of secure applications.

4.6 Release, Operation and Maintenance

- Before the implementation of any new software / digital product, a document covering any security procedures for the new software must be prepared.
- For ready to use software packages, system default settings must be reviewed before installation to determine potential security holes.
- For software packages, all third party supplied default passwords must be changed before the system being placed in a production environment.
- The versioning system should be in place that acts as the source for accountability, the collaboration of source code and revision controller
- Security Control Integration checks shall be performed, and results shall be documented.
- The security controls for digital payment applications must focus on how these applications store, handle and protect payment data. The APIs for secure data storage and communication must be implemented and the security controls must be in line with standards such as OWASP-MASVS, OWASP-ASVS and other relevant OWASP standards, security and data protection guidelines in ISO 12812, threat catalogues and guides developed by NIST (including for Bluetooth and LTE security), for application security and other protection measures. Such testing must necessarily verify for vulnerabilities including, but not limited to OWASP/ OWASP Mobile Top 10, application security guidelines/ requirements developed/ shared by operating system providers/ OEMs.
- Security Certification or accreditation is done to ensure that the controls are effectively implemented through established verification techniques and procedures shall be obtained from third party vendors.
- A deployment review should be performed to ensure that all the security assessments in a different phase of the software development life cycle have been complete, with minimal

residual risk against the final build. A risk profile for each information system development is maintained that specifies the unmitigated security risk with its risk treatment plan.

- Continuous monitoring and an event management system should be in place to ensure all security events in real-time is captured and handled.
- Remove Developer Access account from the production environment.
- Recompile all source code before moving the code into production.
- During the phase, the system performs and the system operations and maintenance, operations assurance shall be responsible for operations and maintenance of the application along with audits and monitoring before it is moved into production.
- The BAU team shall ensure that all security measures are in place.
- A designated team shall document all requisite procedures for operational tasks.
- The system must be continuously checked for any malfunctions/ possible compromise of the system.
- Periodic security assessment (at least annually once) should be done after deployment.
- The Board and Senior Management shall be responsible for the implementation of security controls of the Bank's digital products and services. The policy shall be reviewed periodically, at least on a yearly basis. There will also be an external assessment of the entire process including the logic, build and security aspects of the application(s) supporting the digital product on a yearly basis.
- The Board/ Senior Management i.e. ExCos of bank shall have appropriate performance monitoring systems/ key performance indicators for assessing whether the product or service offered through digital payment channels meet operational and security norms
- Appropriate processes shall be incorporated into the governance and risk management programs for identifying, analyzing, monitoring and managing the specific risks, including compliance risk and fraud risk.

5. Information security essentials

5.1 Security by design

Information security considerations for application services passing over public networks should follow a 'secure by design' approach in the development of digital payment products and services. Barclays shall ensure that digital payment applications are inherently more secure by embedding security within their development lifecycle. For the further information please refer to bank's "Group Information and Cyber Security policy":

5.2 Protecting application services transactions

Information security considerations for application service transactions should include the following:

- Environment, e.g. on a storage platform existing on the organizational intranet, and not retained and exposed on a storage medium directly accessible from the Internet.

- Where a trusted authority is used (e.g. to issue and maintain digital signatures or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process.
- The extent of the controls adopted needs to be commensurate with the level of the risk associated with each form of application service transaction.
- The communication protocol in the digital payment channels should have pertinent encryption and security shall be implemented in the digital payment ecosystem.
- Bank shall redact/ mask customer information such as account numbers/ card numbers/ other sensitive information when transmitted via SMS/ e-mails.
- No sensitive information should be stored by the Web applications of the bank in HTML hidden fields, cookies, or any other client-side storage. Compromise with the data integrity should be strictly avoided.
- The key length (for symmetric/ asymmetric encryption, hashing), algorithms (for encryption, signing, exchange of keys, creation of message digest, random number generators), cypher suites, digital certificates and applicable protocols used in transmission channels, processing of data, authentication purpose, should be robust, adopting internationally accepted and published standards that are not demonstrated to be vulnerable and the configurations involved in implementing such controls are in compliance to extant instructions and the law of the land.
- Effective logging and monitoring capabilities should be in place for digital payments applications, to notify about sudden security changes, malicious user activity, and identify anomalous behavior and transactions.
- Transactions may need to comply with legal and regulatory requirements in the jurisdiction from which the transaction is generated, processed via, completed at or stored.
- Bank's Information Security Group department shall execute automated VA scanning tools to automatically scan all systems on the network that are critical, public-facing or store customer-sensitive data frequently.
- The results from earlier vulnerability scans shall be compared to verify and ascertain that vulnerabilities have been addressed, either by patching, introducing a compensating control, or documenting and accepting the residual risk with obligatory approvals
- Bank shall verify and thoroughly test the functionality (to validate whether the system meets the functional requirements/ specifications) and ensure that security controls of payment products and services are intact and cannot be compromised before its launch in the production environment.
- Bank shall institute a mechanism to actively monitor and look for malicious, rogue, and unauthorized applications.
- Based on the Bank's individual risk/ vulnerability assessment on authentication-related attacks such as brute force/ DoS attacks, Banks shall implement additional levels of authentication to internet banking website such as adaptive authentication, strong CAPTCHA (preferably with anti-bot features) with server-side validation, etc.,
- Bank should ensure that appropriate measures shall be taken to prevent DNS cache poisoning attacks and for secure handling of cookies. Virtual keyboard option should be made available.

5.3 Technical Risk Assessment

Risk and Control self-assessment (RCSA) for digital payment systems should be based on the following criteria:

- Bank shall conduct risk assessments with regard to the safety and security of digital payment products and associated processes and services as well as suitability and appropriateness of the same in relation to the target users, both prior to establishing the service(s) and regularly thereafter. The risk assessment should consider –
    - The technology stack and solutions used,
    - Known vulnerabilities at each of the touchpoints of the digital product and the remedial action taken by the entity,
    - Dependence on third party service providers and oversight over such providers,
    - Risk arising out of integration of digital payment platform with other systems both internal and external to the RE, including core systems and systems of payment systems operators, etc.,
    - The customer experience, convenience and technology adoption required to use such products,
    - Reconciliation process,
    - Interoperability aspects,
    - Data storage, security, and privacy protection as per extant laws/ instructions,
    - Operational risk including fraud risk,
    - Business continuity and service availability,
    - Compliance with extant cyber security requirements; and
    - Compatibility aspects.

    Such assessment shall cover the surrounding ecosystem as well. The assessment of risks shall address the need to protect and secure payment data and evaluate the resilience of systems.
- Bank should conduct the internal Risk and Control Self-Assessment (RCSA) exercise that cover the risks (inherent) & controls in relation to the probability and impact of threats to arrive at residual risk.
- Bank should maintain database of all systems and applications storing customer data in the payment ecosystem and compliance with applicable PCI standards.
- Bank shall evaluate the risks associated with the chosen technology platforms, application architecture, both on the server and client side.
- Bank should undertake a review of the risk scenarios and existing security measures based on incidents affecting their services, before any major change to the infrastructure or procedures is made or, when, any new threats are identified through risk monitoring activities.
- Bank should ensure that unused or unwanted features of the platform should be closely controlled to minimize risk.
- Bank shall develop sound internal control systems and consider the operational risk before offering digital payment products and related services.
- Bank shall ensure that the digital payment architecture is robust and scalable, commensurate with the transaction volumes and customer growth.
- The IT strategy of the bank shall ensure that a robust capacity management plan is in place to meet evolving demand.
- Bank shall also put in place review mechanism of IT/ IT Security architecture and technology platform overhaul on a periodic basis based on Board-approved policy.
- Bank shall have necessary capacity, systems, and procedures in place to periodically test the backed-up data, application pertaining to digital products to ensure recovery without loss of

transactions or audit-trails. These facilities should be tested at least on a half-yearly basis for digital payment products and services.

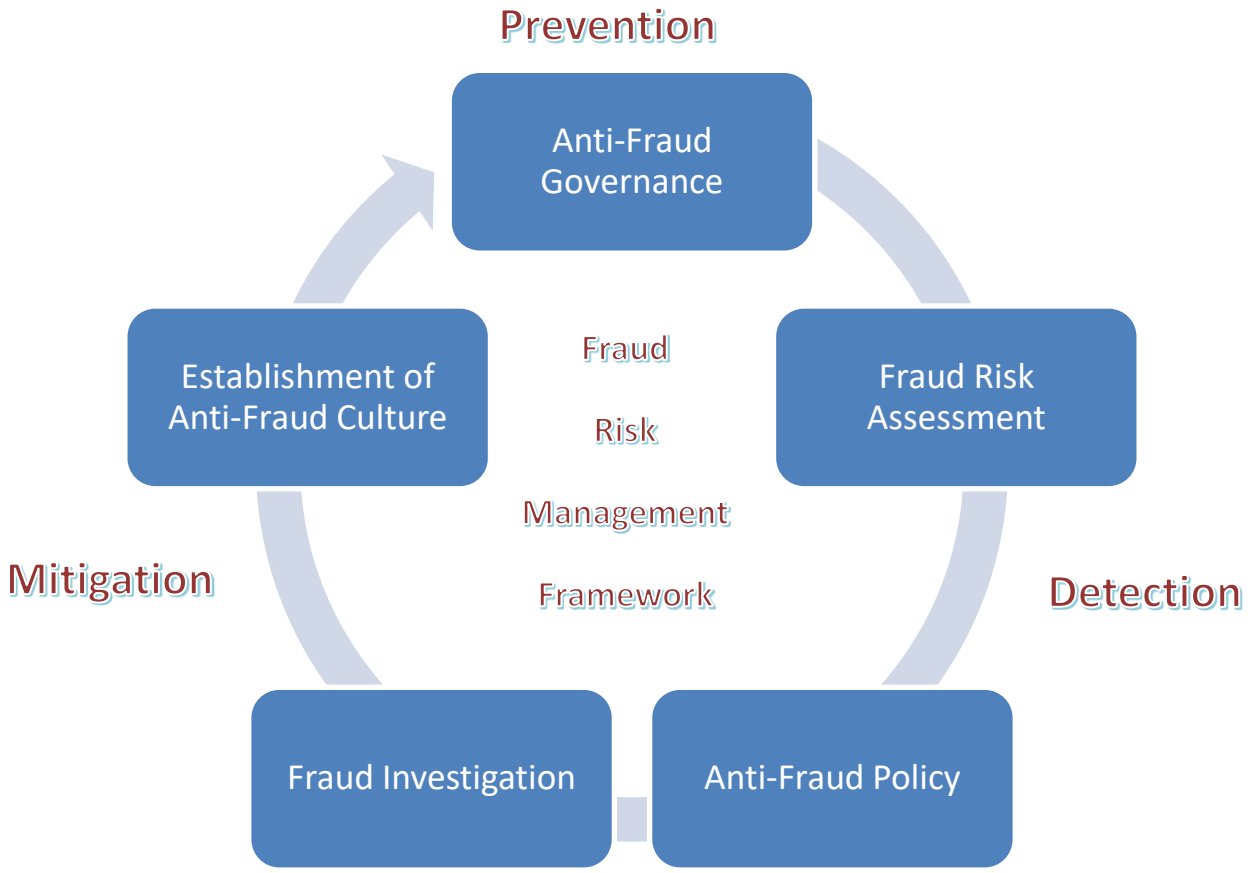
5.4 Authentication Framework for Digital Payment Systems

Bank may also adopt adaptive authentication to select the right authentication factors depending on risk assessment, user risk profile and behavior. The key objectives of multi-factor authentication are to protect the confidentiality of payment data as well as enhance confidence in digital payment by combating cyber-attack mechanisms like phishing, keylogging, spyware/ malware and other internet-based frauds targeted at Banks and their customers.

In this regard,

- Bank should implement appropriate authentication methodologies based on an assessment of the risk posed by the Bank's digital payment products and services.
- Bank should implement an effective authentication method that take into consideration customer acceptance, ease of use, reliable performance, scalability to accommodate growth, customer profile, location, transaction, etc., and interoperability with other systems.
- To enhance online processing security, Bank should implement multi factor authentication and alerts in respect of all payment transactions (including debits and credits), creation of new account linkages (addition/ modification/ deletion of beneficiaries), changing account details or revision to fund transfer limits. In devising these security features, Banks should take into account their efficacy and differing customer preferences for additional online protection.
- Bank should ensure that the alerts and OTPs received by the customer for online transactions shall identify the merchant name, wherever applicable, rather than the payment aggregator through which the transaction was effected.
- Banks should also implement appropriate measures to minimize exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack. This is to ensure that the data in transit is secured and the transactions are authenticated only by genuine/ authorized source/ process.
- Bank should ensure that an authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. In the event of interference or in case the customer closes the application, the session should be terminated, and the affected transactions resolved or reversed out. The customer should be promptly notified about the status of the transaction by email, SMS or through other means.
- Banks should set down the maximum number of failed log-in or authentication attempts after which access to the digital payment product/ service is blocked. Bank should have a secure procedure in place to re-activate the access to blocked product/ service. The customer shall be notified for failed log-in or authentication attempts.
- Bank should ensure automatic termination of online session after a fixed period of inactivity.
- Bank should ensure the secure delivery of password for login. The password generated and dispatched by the Bank should be valid for a limited period from the date of its creation. If the password is generated and dispatched by the Bank, then, the user shall be compulsorily required to change the password, on the first login.

5.5 Fraud Risk Management



The Bank's FRM function has documented and implemented configuration aspects for identifying suspicious and unauthorised transactional behaviour with regards to its Debit cards pool. This is being covered with regards rules triggering cases / alerts, seeking client confirmation where deemed essential, controls such as preventive/ detective in nature etc. Bank monitors alerts generated based on certain parameters. Emails are sent to Clients registered mail id where available to authenticate transaction. Clients may be called on registered no's to seek transaction confirmations. Fraud alert management for client transactions forms part of the "Fraud risk management standard" document.

Barclays Bank as through its current business model in India caters to Local Large Corporates (LLC's) / Global Corporate (GC's) & High Net Worth Individuals. Bank is not involved in High Volume of Internet / Mobile Banking / Cheque / Credit cards transactions which are prone to enormous transactional fraud losses being caused to bank and / or its clients likely through external third parties. Bank has put in enhanced controls via its FCDB portal by activating email / sms alerts for clients to act as a mitigant to any fraudulent activity and this will trigger alerts enabling better controls around client accounts as listed below:

Payment transactions, credit confirmations to remitters & beneficiaries

Credits and debits related to teller transaction, trade and lending transactions, term deposits

Given that there are compensating security (2FA via Gemalto token) and fraud controls are in place from launch via the digital channels and low volume of incremental payment activity, there is already a risk acceptance in place from banks senior management (through ExCo submission)

Bank has a process in place to generate alerts via rules set out for its trivial debit cards portfolio (circa less than # 800) covering various aspects of cash withdrawals / electronic / jewelry / any online transactions/ over high risk MCC; carried out by its clients. Emails are sent to Clients registered mail id where available to authenticate transaction. Clients may be called on registered no's to seek transaction confirmations.

Additionally, in order to mitigate any fraud risk arising through manual processing of fund transfer, requests received vide various modes of payment like original in person, fax, courier/post, email and bearer/messenger, bank has put in place a robust call back process. This is initiated by an independent team from that of payment processing team to have segregation of duties and better controls on the process.

Periodically, the Bank carries out vulnerability scanning as well as penetration tests of its Technology estate, to identify vulnerabilities and ensure that timely patches / remedial measures are applied for the electronic banking system environment including applications, databases and connectivity. Also, it has a 24x7 cyber security monitoring with appropriate tools in place, which helps the Bank to identify and mitigate cyber security threats on time.

- Fraud analysis shall be conducted to identify the reason for fraud occurrence and determine a mechanism to prevent such frauds. This analysis can be documented and saved for future reference.
  - The staff, especially in the fraud control function, shall be aware and educated about fraud. They should be trained in the following skills and areas of expertise:
    - Cardholder and merchant education techniques to prevent fraud.
    - Scheme/ Card operating regulations.
    - Fraud control tools and their usage.
    - Investigative techniques and procedures.
    - Data processing and analysis and liaising or communicating with law enforcement agencies; and
    - The requisite skills required to-
      - Set and update appropriate rules.
      - Monitor the exceptions thrown based on the rules continuously and take necessary actions promptly
      - Communicate/ escalate wherever required to appropriate authorities.
      - Can differentiate false positives from the rest.
  - The FRM function shall maintain updated contact details of service providers, intermediaries, external agencies, and other stakeholders (including other staff) for coordination in incident response. FRM Cell shall put in place a mechanism with the stakeholders to update and verify such contact details. The bank shall also formulate specific SOPs to handle incidents related to the payment ecosystem to mitigate the loss either to the customer or the staff.

5.6 Reconciliation mechanism

A real-time/ near-real-time (not later than 24 hours from the time of receipt of settlement file(s)) reconciliation framework for all digital payment transactions between the Bank and all other stakeholders shall be in place for proactive detection and prevention of suspicious/unauthorized

transactions. A mechanism shall be introduced to monitor the implementation and effectiveness of such a framework.

For the further information please refer to “Reconciliation Policy” established at the bank.

The reconciliation mechanism for such transactions (e.g.- payment system operators, business correspondents, card networks, payment system processors, payment aggregators, payment gateways, third-party technology service providers, other participants, etc.) shall be closely monitored and verified. For the further information please refer to reconciliation process established at the bank.

5.7 Customer protection, Awareness and Grievance Redressal Mechanism

The bank shall formulate a well-documented Customer Grievance and Compensation document and mechanism duly approved by the management.

Following are the parameters to be addressed.

- Introduction of mandatory, secure, safe, and responsible usage guidelines and training materials for end-users within the digital payment applications, with choice of end user-preferred language.
- A mechanism to lodge consumer grievances, with periodic updates. The reporting facility on the application shall provide an option for registering a grievance, and mentioned procedure for customer dispute handling, reporting and resolution procedures, which includes the expected timelines for response and resolution. For the further information please refer to India complaints guideline set by bank.
- Customer awareness about the need to maintain the physical and logical security of their devices accessing digital payment products and services including recommending secure/ regular installation of operating system and application updates, downloading applications only from authorised sources, having anti-malware/ anti-virus applications on devices, etc.
- Customers are provided information about the risks, benefits, and liabilities of using digital payment products and their related services before they subscribe to them.
- Customers awareness programs to enlighten them about their rights, obligations and responsibilities on matters relating to digital payments, and, any problems that may arise from its service unavailability, processing errors and security breaches.

- The terms and conditions including customer privacy and security policy applying to digital payment products and services shall be readily available to customers on demand.
- Customer awareness and training to be held, when new operating features or functions, particularly those relating to security, integrity, and authentication, are introduced to online delivery channels, clear and effective communication followed by sufficient instructions to properly utilise such new features should be provided to the customers.
- Public awareness sessions on the types of threats and attacks used against the consumers while using digital payment products and precautionary measures to safeguard against the same.
- Customers shall be cautioned against commonly known threats in recent times like phishing, vishing, reverse-phishing, remote access of mobile devices and educated to secure and safeguard their account details, credentials, PIN, card details, devices, etc. either via Bank's mail channels, or online advertisements, IVR calls, etc.
- Bank shall provide digital payment products and services, to a customer only at her/ his option based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions.
- The bank should provide a mechanism on their mobile and internet banking application for their customers to, with necessary authentication, identify/ mark a transaction as fraudulent for seamless and immediate notification to his/her Bank/IT Staff. The objective of this mechanism is to accelerate proactive detection and enable the banking/ payment system to trace the transaction trail and mitigate the loss to the defrauded customer at the earliest possible time.

6. Exceptions

Barclays entities shall at all times comply with local regulatory requirements as specified by local regulatory authorities.

Whenever applicable local requirements provide a higher level of requirements for risk assessment or reporting, the Barclays entities and all parties to which these local requirements are applicable shall comply with the higher level of protection, on top of the rules and provisions laid down in this Policy.

Exceptions shall be granted only when the following criteria are met:

- There is a real security necessity or compelling situation supported by appropriate due diligence and adequate controls;
- There is a lack of a reasonable alternative

Exceptions to this policy must be handled according to the processes and requirements satisfying the Dispensations Waivers and Breaches Standard.

7. Appendices

Related Documentation – Policies and Standards

Document Type	Document Name
Standards	Group NAPA Standard and Product Review Group wide standard
	Control Environment and Risk Profile Assessment(CERPA) Standard
	Third Party Service Provider Management Standard
	Customer Complaints and Remediation Standard
	Fraud Management Standard
	Dispensations Waivers and Breaches Standard
Policies	Information and cyber security policy
	Technology Risk Policy

8. RACI Matrix

Activities	CISO	App Sec Team	App Dev Team	Legal / Compliance	Product process approval committee
Introduction of a new digital payment product	C/I	C	R	C/I	A
Changes/upgrades of the digital payment product	C	C	R	C/I	A

---------- End of Document ----------