

P E R S P E C T I V E

Check Frauds

Lines of Defense in Integrated
Payments Module



YOUR INNOVATION PARTNER

Payments frauds have been pain points for banks and customers from the reputational, legal and financial risk aspects. With roll out of Basel II norms on operational risks, payments operational risk carries capital charge also. In this context, banks need to implement and establish strong lines of defense to combat payment frauds. Lines of defense offered by integrated payments module within core banking system are discussed here specifically with check frauds in focus. The objective is to provide trusted applications, which enables banks to offer “Fraud-Free” environment to their clientele.

Payments Fraud – Scrolling Numbers

Basel II guidelines define operational risk as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Inadequate process, people and system creates vulnerability and exposed vulnerability results in risk of loss. Payments risk results in financial loss, reputational loss and even systemic failures of institutions. Annual surveys on payments fraud indicate that an increasing number of organizations have been victims of frauds, and the incidences of fraud increases every year. With the disruptive evolution of payment methods and channels, commoditization of payment offerings, emergence of APP (Alternate Payment Providers), vulnerabilities are created and exposed, pushing stakeholders to higher risks. Risk combating modes adopted by financial institutions are based on preventive, punitive and avoidance strategies. Avoidance decision will be calculated and planned where organization deliberately decides to face the impact if occurred, due to high costs involved in combat, low impact on business and low probability of occurrence. To minimize or mitigate risks, organizations do expect payment providers to have robust systems in place to assist them in combating the possible fraud attacks / intrusions into their payment processes.

Integrated Core Banking Payments

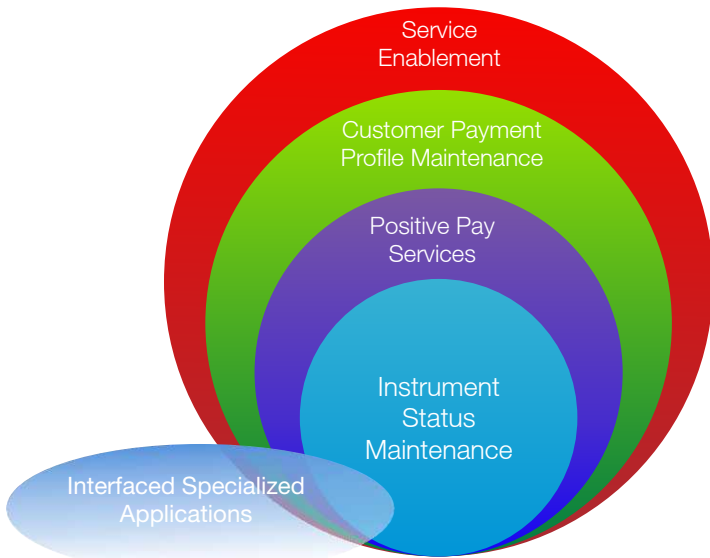
Given the expectations of bank customers to ensure safe and secure payments, banks have opportunities to showcase the capabilities of payment engines to clientele and edge out competition by meeting not merely today's requirements but providing capabilities which can scale up with minimal technical interventions and costs to meet future requirements as well. There is always a choice between a best of breed and an integrated solution, the pros and cons of the same have been dissected by analysts multiple times.

Focusing on advantages of integrated payments capabilities within core banking systems, replacing multiple siloed complex legacy systems, have definite advantages in combating payment frauds, given the integration with customer information, account information, transaction history, inventory control, debit authorizations in centralized environment. Various lines of defense against payment frauds, do enable financial institutions to offer broad coverage in this area, without slicing combat functionalities to multiple back end applications with little synchronization.

Check Fraud Controls

Though traction towards electronic payment modes is evident in almost all geographies, with certain geographies completely moved into electronic regime, the share of checks in payment volumes in today's environment is still to be reckoned with. Fraud, such as counterfeiting or check forgery, has always had a global reach. However, it is observed that payments fraud used to be much more reliant on physical connections between parties, such as the theft of an individual checkbook earlier. Now with sophisticated duplication mechanisms and fraud methodologies, banks need to build up the lines of defense in check processing applications. Understanding life cycle of check processing, will enable banks to identify points of fraud control. Following lines of defense are identified in check processing capabilities offered by integrated payments module, to meet challenges in this domain.

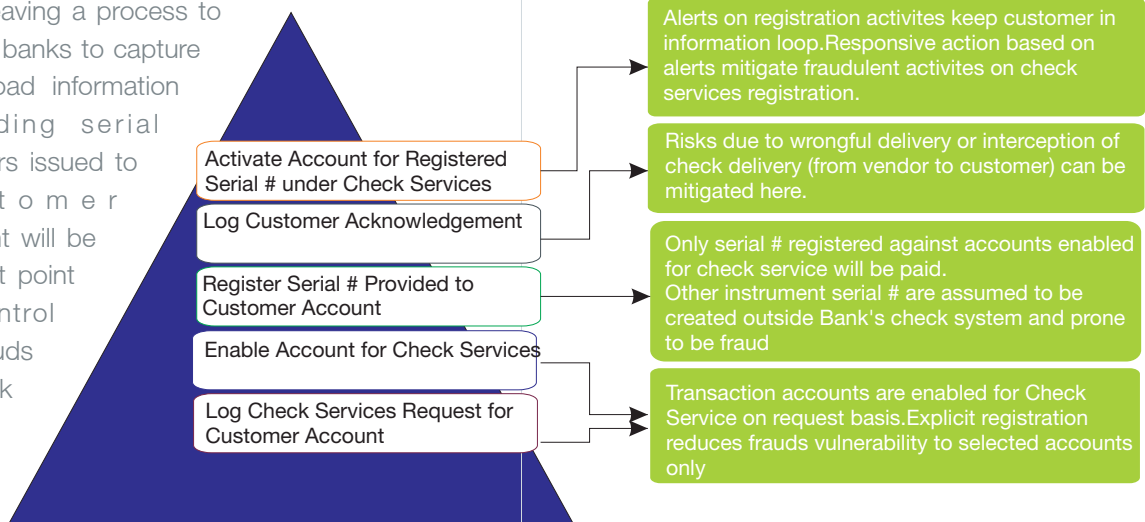
- Service enablement
- Customer payment profile maintenance
- Positive pay services
- Instrument status monitoring
- Interfaced specialized applications



Source : Infosys Technologies Limited

First Line of Defense - Service Enablement Controls

As a process, banks need to be completely involved and make their systems aware of the check service enablement process and stages. A typical process which would be able to mitigate risks involved during payment of check not issued by customer, serial number not belonging to customer, vendor risks, interception of check book in vendor–customer interactions, among others can be addressed through this process. This process is typically not practiced in few geographies since the process of check printing and delivery is outsourced to external agencies, wherein bank acts as a facilitator in the process without information on check details flowing from outsourced vendor to customer. Interweaving a process to enable banks to capture or upload information regarding serial numbers issued to customer account will be the first point of control for frauds at bank level.



Second Line of Defense – Payment Profile Maintenance

Every customer is unique in their business operations and needs. Banks need to identify and to the extent possible capture customer preferential to differentiate one from other. The differentiation will clearly be the plank for better fraud management also. Blind eyed fraud attempts by external entities/Intruders will be futile at business firewalls jointly set by customer and bank.

Customer level payment profiles at bank level will achieve the following objectives from fraud

Bank logs customer request for check service

Bank registers account for check service. Risk addressed: Only one account enabled for check service, inward checks will be paid. First level of fraud controls

Vendor arranges for check book and mails to customer. Vendor parallelly advises bank of the serial # used in the forwarded check books along with account bank adds on check information to account. Risk Addressed: Only those instrument serial # sent to customer will be honoured through the account. Second level of fraud control after account subscription.

Customer acknowledges receipt of check book from vendor. Bank updates acknowledgement in system. Risk Addressed: Check book received at wrong hands will be tackled here since customer secured identification will be done during registration of acknowledgement

- Define exceptions within boundaries
 - Payment against instruments not issued instrument
 - Amount mismatch
 - Date mismatch
 - Stale instrument
 - Stopped instruments
 - Payee mismatch
- Automation parameters to handle volumes
 - Straight Through Processing(STP) limits
 - Overriding exceptions (of negligible impact to business)

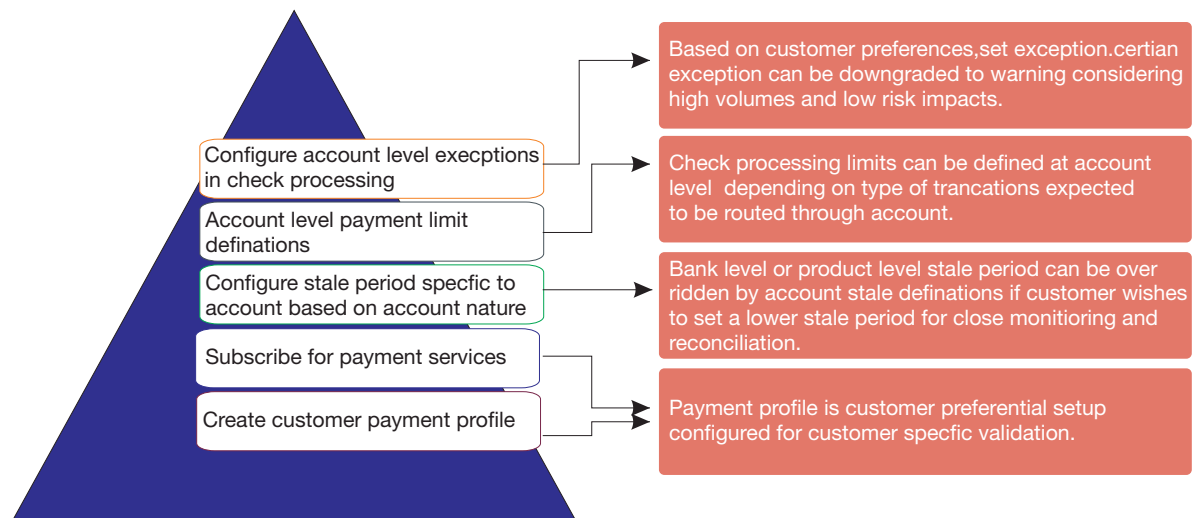
Strength of integration with core banking functionalities is at its peak in this line of defense with full account information and properties available to payment operations for defining preferential on exception management, inventory management, account management, and accounting transaction management. Unified handling of payment across multiple payment systems will be another strong point of integrated payments module. In siloed payment operations, this would be a challenge considering interfacing capabilities of such application, identification of base referential information and standardization of common interchange formats. In practice, siloed applications are maintaining application specific customer information for such validations, losing on the unified view on customer and centralized customer profile maintenance. Integrated payments module will be reposing on centralized customer profile, maintained at bank level as a shareable service for all departments within bank and payment schemes.

Third Line of Defense – Positive Pay Services

'Positive Pay' is reckoned as one of the effective check fraud combat tool by customers, since customer is in loop of payment till funds move out the drawer account. Every decision taken at bank is transparent to customer in the process. Bank refers any exception encountered during check processing to customer for validations. Customer confirms decision to Pay or No Pay after verifying the presented instrument details with the payable information available in their accounting applications. Banks then apply customer's decision on the exception item. The touch-point is before actual funds movement out of customer account and hence customer has last say on the funds disposition. Coupled with account reconciliation services and channel offerings by banks, customers accounting books are almost synchronized with the account activities in bank books.

In positive pay subscription, customer can register different exception preferences depending on account nature. Set of common validations done as part of positive pay services are:-

- Instrument not found in issuance records
- Amount mismatch
- Instrument date mismatch
- Payee mismatch
- Instrument status – stale
- Instrument status – cancelled
- Instrument status – caution
- Instrument status - stop





YOUR INNOVATION PARTNER

PERSPECTIVE

Universal Banking Solution | System Integration | Consulting | Business Process Outsourcing

Infosys Technologies Limited

Plot No. 44, Electronics City, Hosur Road, Bangalore - 560100, India.
Tel.: + 91 80 28520261, Fax: + 91 80 28521747, e-mail: finacleweb@infosys.com
www.infosys.com/finacle

"COPYRIGHT NOTICE: Copyright ©2009 Infosys Technologies Limited, Bangalore, India. ALL RIGHTS RESERVED."
Finacle logo is a registered trademark of Infosys and Infosys acknowledges the proprietary rights of the trademarks and product names of other companies mentioned in this document. Infosys believes the information in this publication is accurate as of its publication date; such information is subject to change without notice.