Mobile Money in Jamaica

mconec
Mobile Payment Services

Kavin Hewitt
CEO
MCONEC Mobile Payment Services

Agenda

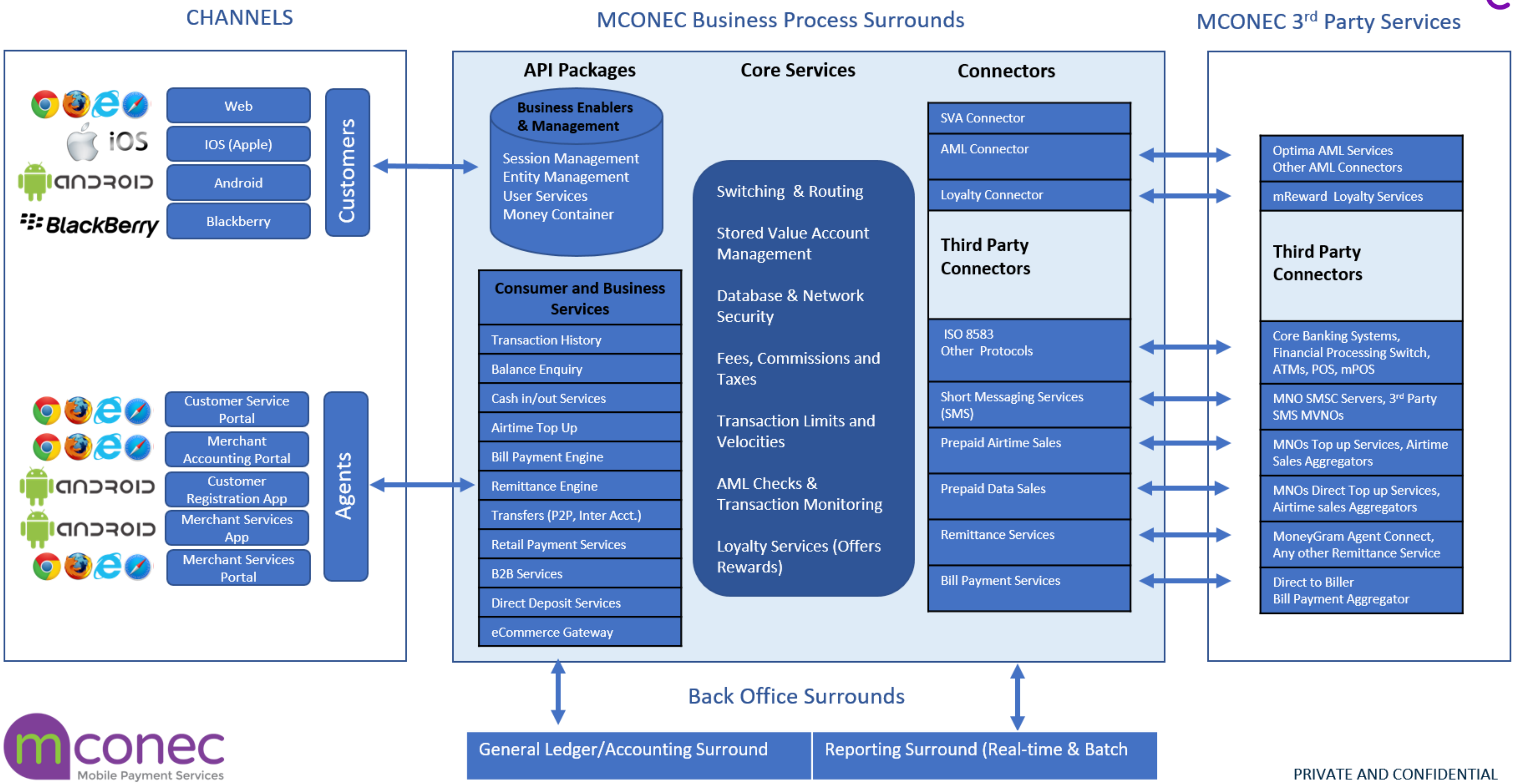
- Mobile Money vs Mobile Wallet
- The Mobile Wallet Ecosystem
- Suite of Services
- BOJ Requirements & Technology Impact
- Consumer Security & Privacy
- Secure Infrastructure – Network & Host

Mobile Money Vs Mobile Wallet

- Mobile money is digitized cash made further accessible on mobile devices
  - No different from money held at a bank or on a card or other instrument of stored value
- Mobile money is a component of the Mobile Wallet
- Mobile money exists within an ecosystem

- The Mobile Wallet is a secure digital container wherein value can be stored and retrieved within the context of an ecosystem
- Value may be represented by:
  - Cash
  - Cards
  - Coupons
- Accessibility and Security are key factors

The Mobile Wallet Ecosystem - CONEC



CHANNELS

Web
IOS (Apple)
Android
Blackberry
Customers

Customer Service Portal
Merchant Accounting Portal
Customer Registration App
Merchant Services App
Merchant Services Portal
Agents

MCONEC Business Process Surrounds

API Packages

Business Enablers & Management

Session Management
Entity Management
User Services
Money Container

Consumer and Business Services

- Transaction History
- Balance Enquiry
- Cash in/out Services
- Airtime Top Up
- Bill Payment Engine
- Remittance Engine
- Transfers (P2P, Inter Acct.)
- Retail Payment Services
- B2B Services
- Direct Deposit Services
- eCommerce Gateway

Core Services

- Switching & Routing
- Stored Value Account Management
- Database & Network Security
- Fees, Commissions and Taxes
- Transaction Limits and Velocities
- AML Checks & Transaction Monitoring
- Loyalty Services (Offers Rewards)

Connectors

- SVA Connector
- AML Connector
- Loyalty Connector

Third Party Connectors

- ISO 8583 Other Protocols
- Short Messaging Services (SMS)
- Prepaid Airtime Sales
- Prepaid Data Sales
- Remittance Services
- Bill Payment Services

MCONEC 3rd Party Services

- Optima AML Services Other AML Connectors
- mReward Loyalty Services

Third Party Connectors

- Core Banking Systems, Financial Processing Switch, ATMs, POS, mPOS
- MNO SMSC Servers, 3rd Party SMS MVNOs
- MNOs Top up Services, Airtime Sales Aggregators
- MNOs Direct Top up Services, Airtime sales Aggregators
- MoneyGram Agent Connect, Any other Remittance Service
- Direct to Biller Bill Payment Aggregator

Back Office Surrounds

General Ledger/Accounting Surround

Reporting Surround (Real-time & Batch

Mobile Payment Services

PRIVATE AND CONFIDENTIAL

Customer Suite of Services

AIRTIME TOP UP

Subscribers can instantly add credit (air-time) to their mobile phone or any other pre-paid mobile phone. Recipients can be saved for easy future top ups

BALANCE ENQUIRIES

Subscribers can check balances on their Stored Value Accounts (SVA) or their connected Bank or Credit Union accounts

BILL PAYMENTS

Subscribers can pay bills to companies registered on the system for bill payment e.g. Utility companies

CASH IN/CASH OUT

This feature allow subscribers to add cash to their wallet or withdraw cash from their wallets at registered agents or merchants

INTER-ACCOUNTS BANK TRANSFERS TO WALLET

This feature allows the subscriber to transfer from their SVA to the their bank or prepaid card account or vice versa

PERSON TO PERSON TRANSFER

The subscriber can transfer from their SVA to another subscriber's SVA

RETAIL PAYMENTS

This feature allows subscribers to pay for goods or services using their mobile wallet. Payment may be made from the SVA or any connected account.

INTERNATIONAL REMITTANCE TRANSFER

Subscribers can pull down remittances to their Stored Value Account (SVA) or their connected Credit Union or Bank Account

Corporate Suite of Services

AIRTIME TOP UP

This feature allows the agent/merchant to sell prepaid airtime to cash customers via the MCONEC merchant portal

BALANCE ENQUIRIES

This feature allows the agent/merchant to check the balance on their Stored Value Accounts (SVAs)

BILL PAYMENTS

Agents/Merchants can accept cash bill payments for companies registered on the system for that service e.g. Utility companies

CASH IN/CASH OUT

This feature allows registered agents or merchants to receive or pay out cash from registered subscribers, Agents or Merchants

MVAULT - BUSINESS TO BUSINESS TRANSFERS

This feature allows merchants or agents to raise and settle invoices to another merchant or agent (B2B, G2B)

DIRECT DEPOSIT

deposit cash onto many wallets

Corporations can transfer from their SVAs to multiple subscriber's SVAs. E.g. Payroll, benefits and refunds

RETAIL PAYMENTS

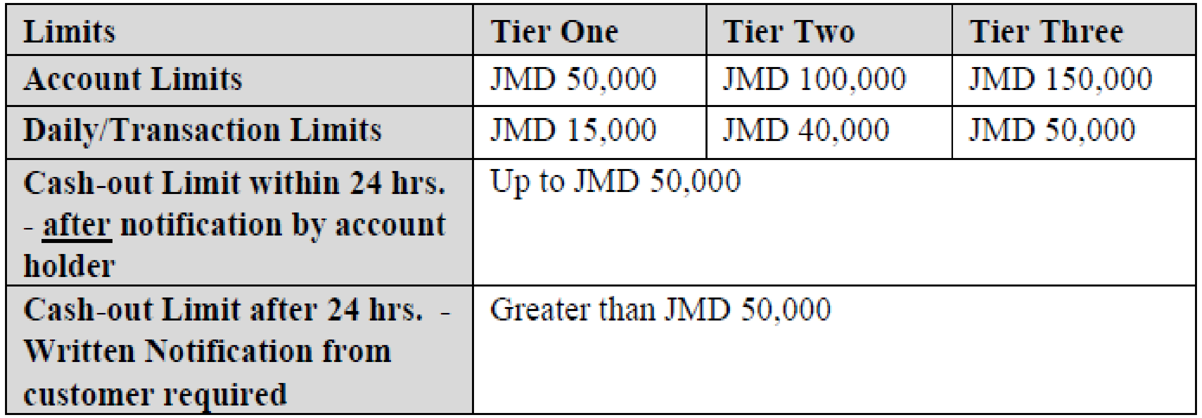
This feature a merchant to receive payment for goods or services from registered subscribers via the merchant portal or app.

eCommerce Payment Gateway

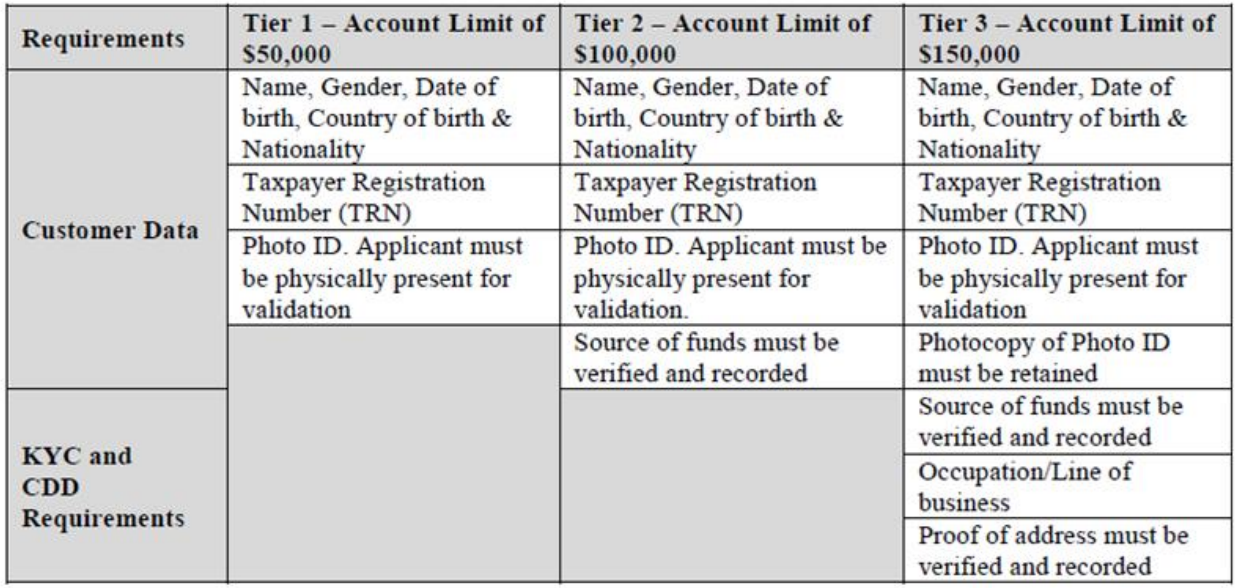
This feature provides an interface where merchants can sell and accept payments from subscribers online or via mobile applications.

BOJ Requirements & Technology Impact

- 3 Tier Requirement in Jamaica
  - Account upper limits by tiers
  - Transaction upper limit by tiers
  - KYC requirement by tiers
- The system allows Multi-tiers (n+1)
- The system allows KYC by tiers
- Each transaction must pass several checks prior to being processed
  - Account and transaction limits
  - Product velocity checks
- Major resource "hog" on the system



Limits	Tier One	Tier Two	Tier Three
Account Limits	JMD 50,000	JMD 100,000	JMD 150,000
Daily/Transaction Limits	JMD 15,000	JMD 40,000	JMD 50,000
Cash-out Limit within 24 hrs. - after notification by account holder	Up to JMD 50,000		
Cash-out Limit after 24 hrs. - Written Notification from customer required	Greater than JMD 50,000		

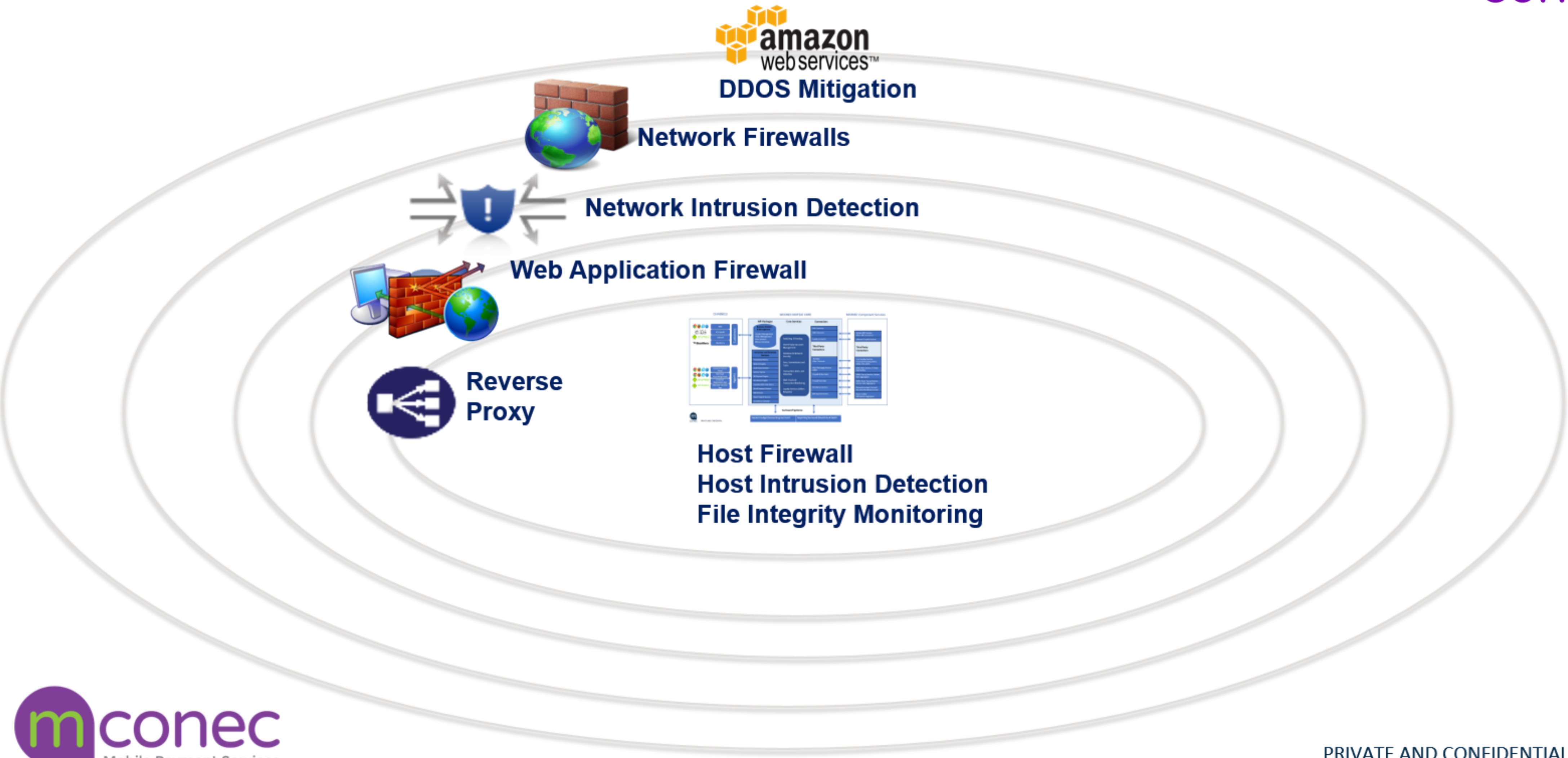


Requirements	Tier 1 – Account Limit of $50,000	Tier 2 – Account Limit of $100,000	Tier 3 – Account Limit of $150,000
Customer Data	Name, Gender, Date of birth, Country of birth & Nationality	Name, Gender, Date of birth, Country of birth & Nationality	Name, Gender, Date of birth, Country of birth & Nationality
	Taxpayer Registration Number (TRN)	Taxpayer Registration Number (TRN)	Taxpayer Registration Number (TRN)
	Photo ID. Applicant must be physically present for validation	Photo ID. Applicant must be physically present for validation.	Photo ID. Applicant must be physically present for validation
		Source of funds must be verified and recorded	Photocopy of Photo ID must be retained
KYC and CDD Requirements			Source of funds must be verified and recorded
			Occupation/Line of business
			Proof of address must be verified and recorded

Customer Security and Privacy

- Payment Application & Payment Card Industry Data Security Standards
- Data driven transaction using secure protocols via apps &/or Web Portals
- Scalability and Redundancies considered
- Real Time transaction monitoring
  - Watchlist Scanning
  - Alerts
  - Trend monitoring
    - Geographic
    - Behavioural
- Multi- Factor Security
  - Password + PIN for transaction
  - Customer self activates account and sets up credentials

Secure Infrastructure – Network & Host



amazon web services™

DDOS Mitigation

Network Firewalls

Network Intrusion Detection

Web Application Firewall

Reverse Proxy

Host Firewall
Host Intrusion Detection
File Integrity Monitoring

PRIVATE AND CONFIDENTIAL

Network & Host Security Detailed

1. **Network**
    - Network ACLs (Amazon ACLs)
    - Network Firewalls
    - Network Intrusion Detection
    - Web Application Firewalls
    - Forward/Reverse Proxy Servers

2. **Server**
    - CIS/NIST Hardened servers (CentOS)
    - Host Firewalls (IP Tables)
    - Host Intrusion Detection
    - File Integrity Monitoring
    - Configuration Management
    - Central Logging/Correlation
      (Security Event and Incident Mgmt.)

3. **Application**
    - CIS/NIST Hardened applications
      (Tomcat, PostgreSQL)
    - Central Logging/Correlation
      (Security Event and Incident Mgmt.)

4. **Platform**
    - Role-based security
    - Password/PIN protection
      (session token, password/PIN hashed)
    - Encrypted PAN and cardholder data
    - Replace all reference to PAN and account data with a token
    - Audit and logging

5. **Development and Operational Procedures**
    - Training on OWASP Top 10 and coding best practices
    - Automated testing for all software updates
    - Manual code reviews
    - Automated code reviews for OWASP Top 10
      (3rd Party)
    - Network scanning both from internal and external networks
    - Penetration testing (3rd Party)
    - PCI Scanning (3rd Party)

Discussion