Developmental Imperatives of Mobile Money and Implications on Security

Thabiso MOERANE
March 2012
The proliferation of Mobile Money services, particularly “Person-to-Person Transfer Services” provide a foundation for Developing Countries to promote Financial Inclusion. Financial Inclusion requires a formal financial system that can be trusted by the users. Service Providers of Mobile Money services are, or at least should be, considered part of the formal financial system. This is because the operation of the formal financial system is profoundly important for economic growth and poverty alleviation. It influences how many people are hungry, homeless, and in pain. It shapes the gap between the rich and the poor. It arbitrates who can start a business and who cannot, who can pay for education and who cannot, who can attempt to realize one’s dreams and who cannot (WEF, 2008)...

The challenge facing Mobile Money Service Providers in Developing Countries is finding a balance amongst dynamics that are seemingly in conflict:

“Affordability; Relevant Service; Customer Experience and Security...”
Contents

- Background
- Financial Inclusion: Main Requirements
- Nigeria Market Profile
- Mobile Banking/Payments Regulatory Framework in Nigeria
- Service Description
- Customer Experience
- Security
- Conclusion
- Questions
Financial Inclusion

Main Requirements
Minimum Services Required to Achieve Financial Inclusion

1. **Savings** – This is more about enabling people to have a safe place to keep money.
2. **Payments** – An ability for people to make payments in a safe, accessible and affordable manner.
3. **Insurance** – A basic insurance service such as a basic funeral policy; and
4. **Credit** – Access to credit. People don’t accumulate assets from savings but from access to credit.

A facility that enables records of **Savings** and **Payments** creates a record of **Transaction History** that enables FIs to build a **Financial History** of customers such that they can develop further products suitable for the target market.
Socially Desirable Outcomes

**Financial Development:** The efficiency of the financial system as a payments mechanism and intermediation system is maximised and in turn, contribute to overall economic growth.

**Financial Stability:** The safety and soundness of the banking and payments system is not compromised.

**Financial Integrity:** The service should not compromise the financial system through abuse for criminal and terrorist financing purposes

**Financial Inclusion:** Financial Inclusion is delivering affordable financial services to the vast sections of the disadvantaged and low income groups.

**Consumer Protection:** The customers must enjoy adequate protection as provided for by legislation
Nigeria Market Profile

Affordability and Market Size
Mobile Banking Target Market

- **Fully-Banked**
  Services by Branch-Centric Model and Internet Banking

- Mobile Banking Target Market
  Currently un/under-banked

- Financially Included:
  - Fully Banked
    - 25.4 million

- Other Formal Financial Services:
  - Unbanked
    - 5.3 million

- Financially Excluded:
  - Informal Financial Services
    - 14.8 million

- Financially Excluded:
  - Unbanked
    - 39.2 million

Source: EFnA, 2010
Barriers to Banking in Nigeria

- The main barriers to banking in Nigeria are irregular income, unemployment and distance, particularly in rural areas.

<table>
<thead>
<tr>
<th>Barriers</th>
<th>TOTAL</th>
<th>URBAN</th>
<th>RURAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Irregular income</td>
<td>47.5%</td>
<td>46.7%</td>
<td>47.7%</td>
</tr>
<tr>
<td>Unemployed</td>
<td>33.6%</td>
<td>33.4%</td>
<td>33.6%</td>
</tr>
<tr>
<td>Too far</td>
<td>27.2%</td>
<td>10.9%</td>
<td>31.7%</td>
</tr>
<tr>
<td>Illiterate</td>
<td>13.7%</td>
<td>7.3%</td>
<td>15.5%</td>
</tr>
<tr>
<td>Transport costs</td>
<td>13.2%</td>
<td>6.9%</td>
<td>15.0%</td>
</tr>
<tr>
<td>Expensive</td>
<td>9.7%</td>
<td>10.2%</td>
<td>9.6%</td>
</tr>
<tr>
<td>Lack of trust</td>
<td>8.3%</td>
<td>8.5%</td>
<td>8.2%</td>
</tr>
<tr>
<td>Too much documentation</td>
<td>5.8%</td>
<td>7.8%</td>
<td>5.2%</td>
</tr>
</tbody>
</table>

Source: EFInA, 2010
## Nigeria Demographics: Affordability

<table>
<thead>
<tr>
<th>Adult Population (18+ years)</th>
<th>84,700,000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Affordability</strong></td>
<td><strong>32.3%</strong></td>
</tr>
<tr>
<td><strong>Exchange Rate</strong></td>
<td><strong>151.774</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monthly Income Levels*</th>
<th>Population*</th>
<th>%age of Population*</th>
<th>Maximum Income per Level*</th>
<th>Affordable Bank Fees pm</th>
<th>Affordable Bank Fees pm</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSM 1 Don't Know</td>
<td>18,125,800</td>
<td>21.4%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSM 1 No Income</td>
<td>9,232,300</td>
<td>10.9%</td>
<td>NGN 0</td>
<td>NGN 0</td>
<td>$0</td>
</tr>
<tr>
<td><strong>Sub-Total</strong></td>
<td><strong>27,358,100</strong></td>
<td><strong>32.3%</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSM 1 &lt;N250</td>
<td>1,694,000</td>
<td>2.0%</td>
<td>NGN 250</td>
<td>NGN 5</td>
<td>$0.03</td>
</tr>
<tr>
<td>LSM 2 N251-N1,000</td>
<td>3,472,700</td>
<td>4.1%</td>
<td>NGN 1,000</td>
<td>NGN 20</td>
<td>$0.13</td>
</tr>
<tr>
<td>LSM 3 N1,000-N2,000</td>
<td>6,437,200</td>
<td>7.6%</td>
<td>NGN 2,000</td>
<td>NGN 40</td>
<td>$0.26</td>
</tr>
<tr>
<td>LSM 4 N2,001-N6,000</td>
<td>8,385,300</td>
<td>9.9%</td>
<td>NGN 6,000</td>
<td>NGN 120</td>
<td>$0.79</td>
</tr>
<tr>
<td>LSM 5 N6,000-N13,000</td>
<td>10,248,700</td>
<td>12.1%</td>
<td>NGN 13,000</td>
<td>NGN 260</td>
<td>$1.71</td>
</tr>
<tr>
<td><strong>Weighted Average Affordability</strong></td>
<td><strong>30,237,900</strong></td>
<td><strong>35.7%</strong></td>
<td></td>
<td>NGN 132</td>
<td>$0.87</td>
</tr>
<tr>
<td>LSM 6 N13,001-N20,000</td>
<td>7,961,800</td>
<td>9.4%</td>
<td>NGN 20,000</td>
<td>NGN 400</td>
<td>$2.64</td>
</tr>
<tr>
<td>LSM 7 N20,001-N40,000</td>
<td>5,166,700</td>
<td>6.1%</td>
<td>NGN 40,000</td>
<td>NGN 800</td>
<td>$5.27</td>
</tr>
<tr>
<td>LSM 8 N40,001-N70,000</td>
<td>2,710,400</td>
<td>3.2%</td>
<td>NGN 70,000</td>
<td>NGN 1,400</td>
<td>$9.22</td>
</tr>
<tr>
<td>LSM 9 N70,001-N100,000</td>
<td>592,900</td>
<td>0.7%</td>
<td>NGN 100,000</td>
<td>NGN 2,000</td>
<td>$13.18</td>
</tr>
<tr>
<td>LSM 10 &gt;N100,000</td>
<td>592,900</td>
<td>0.7%</td>
<td>NGN 100,000</td>
<td>NGN 2,000</td>
<td>$13.18</td>
</tr>
<tr>
<td>Refused to Answer</td>
<td>10,164,000</td>
<td>12.0%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>27,188,700</strong></td>
<td><strong>32.1%</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **Total**              | **84,784,700** | **100.1%**          |                           |                         |                         |

**Sources:** EFINA*; Finmark Trust**; Oanda***

---

AT THE SPEED OF IDEAS™

COPYRIGHT © 2011 ALCATEL-LUCENT. ALL RIGHTS RESERVED.
Mobile Banking/Payments Regulatory Framework in Nigeria

In Compliance with the Central Bank of Nigeria (CBN) Regulatory Framework for Mobile Payment Services in Nigeria
# Nigeria Regulatory Framework: Models & Services

<table>
<thead>
<tr>
<th>Bank-Focused (Banks Only)</th>
<th>Bank-Led (Consortium)</th>
<th>Non-Bank-Led</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Participants</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initiating Bank</td>
<td>Initiating Bank/s</td>
<td>Corporate Organisation</td>
</tr>
<tr>
<td>ICT Partner/s</td>
<td>Partner Organisations</td>
<td>Partner/s</td>
</tr>
<tr>
<td></td>
<td>Scheme Operator/s</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MNOs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Independent Operator/s</td>
<td></td>
</tr>
<tr>
<td><strong>Mobile Payment Scenarios</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bank Account-Based</td>
<td>Card Account-Based</td>
<td>System-Based (SVA)</td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide all m-Payment services</td>
<td>Provide all financial services</td>
<td>Provide and manage technology</td>
</tr>
<tr>
<td>Facilitate International Remittances</td>
<td>Provide and manage technology</td>
<td>Provide Agent Network</td>
</tr>
<tr>
<td></td>
<td>Provide Agent Network</td>
<td>Facilitate International Remittances</td>
</tr>
<tr>
<td></td>
<td>Facilitate International Remittances</td>
<td></td>
</tr>
</tbody>
</table>
Service Description

Mobile Payment Service
Mobile Money is NOT an end in itself but a means to an end, which is enabling m-Commerce by enabling m-Payments for services...
Therefore, there are only two types of payments: Proximity and Remote...

**Proximity Payments**
- Cash-In/Cash-Out
- Retail Purchases
- Bill Payment through Retailer (Agent)
- Money Transfer through Retailer (Agent) – Domestic
- Pre-Paid Services: Top-Up through Retailer (Agent) – Airtime, Electricity, Water

**Remote Payments**
- Bill Payment
- Money Transfer – Domestic
- Pre-Paid Services: Top-Up – Airtime, Electricity, Water

The only difference between a proximity and a remote payment is that the proximity payment involves a retailer (who is either an agent or a merchant or BOTH) whereas a remote payment doesn’t!
Customer Experience
THE CUSTOMER JOURNEY (m-Commerce): TOUCHPOINT MAP

1. AWARENESS
   • Brand image: personality

2. INTERACT
   • Service promise
   • Selection and value

3. AGREE/GET
   • Discover: easy to find, search, recommend (e.g., portal)
   • Channels: store, portal, CSR
   • Easy registration as customer
   • Activate: easy to buy, quick and easy services delivery
   • Personalize: bundle, flexibility

4. CONSUME
   • Perceived service quality
   • Change, add, and services
   • Simple and easy to modify account (e.g., add members modify privileges)

5. USE
   • Problem, question, change interaction
   • Self serve, CSR, IVR: portal, chat, phone, social
   • Information availability
   • Authority to fix

6. PAY
   • Billing and reporting: paper, electronic
   • Understand
   • Self service
   • Payment options

7. REWARD
   • Loyalty program

8. LEAVE
   • Easy and friendly
   • Keep record for ease of return

Source: Alcatel Lucent, 2012
Security

Open Web Application Security Project (OWASP)
Top 10 Mobile Risks

Source: OWASP, 2011
Mobile Threat Model
Mobile Threat Model

**Spoofing**
- Improper Session Handling
- Malicious QR Code
- Untrusted NFC Tag Or Peer

**Tampering**
- Modifying Local Data
- Weak Authentication
- Carrier Network Breach
- Insecure WiFi network

**Information Disclosure**
- Malicious Authentication
- Reverse Engineering Apps
- Backend Breach
- Push Apps Remotely

**Repudiation**
- Weak Authorization
- Client Side Injection
- Make Unauthorized Purchases

**Denial of Service**
- Malware
- Crashing Apps
- Push Notification Flooding
- Excessive API Usage

**Elevation of Privilege**
- Malware
- Toll Fraud
- Sandbox Escape
- Compromised Credentials
- Compromised Device
- Rootkits
## Top 10 Risks

<table>
<thead>
<tr>
<th>OWASP Mobile Top 10 Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>M1- Insecure Data Storage</strong></td>
</tr>
<tr>
<td><strong>M2- Weak Server Side Controls</strong></td>
</tr>
<tr>
<td><strong>M3- Insufficient Transport Layer Protection</strong></td>
</tr>
<tr>
<td><strong>M4- Client Side Injection</strong></td>
</tr>
<tr>
<td><strong>M5- Poor Authorization and Authentication</strong></td>
</tr>
</tbody>
</table>
M1- Insecure Data Storage

- Sensitive data left unprotected
- Applies to locally stored data + cloud synced
- Generally a result of:
  - Not encrypting data
  - Caching data not intended for long-term storage
  - Weak or global permissions
  - Not leveraging platform best-practices

Impact

- Confidentiality of data lost
- Credentials disclosed
- Privacy violations
- Non-compliance
M1- Insecure Data Storage

Prevention Tips

- Store ONLY what is absolutely required
- Never use public storage areas (ie- SD card)
- Leverage secure containers and platform provided file encryption APIs
- Do not grant files world readable or world writeable permissions

<table>
<thead>
<tr>
<th>Control#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1-1.14</td>
<td>Identify and protect sensitive data on the mobile device</td>
</tr>
<tr>
<td>2.1, 2.2, 2.5</td>
<td>Handle password credentials securely on the device</td>
</tr>
</tbody>
</table>
M2- Weak Server Side Controls

OWASP Top 10

- https://www.owasp.org/index.php/Category:OWASP Top Ten Project

OWASP Cloud Top 10


- R1: Accountability & Data Risk
- R2: User Identity Federation
- R3: Regulatory Compliance
- R4: Business Continuity & Resiliency
- R5: User Privacy & Secondary Usage of Data
- R6: Service & Data Integration
- R7: Multi-tenancy & Physical Security
- R8: Incidence Analysis & Forensics
- R9: Infrastructure Security
- R10: Non-production Environment Exposure
M2- Weak Server Side Controls

Prevention Tips

- Understand the additional risks mobile apps introduce into existing architectures
- Leverage the wealth of knowledge that is already out there
- OWASP Web Top 10, Cloud Top 10, Web Services Top 10
- Cheat sheets, development guides, ESAPI

<table>
<thead>
<tr>
<th>Control#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1-5.8</td>
<td>Keep the backend APIs (services) and the platform (server) secure</td>
</tr>
</tbody>
</table>
M3- Insufficient Transport Layer Protection

- Complete lack of encryption for transmitted data
  - Yes, this unfortunately happens often
- Weakly encrypted data in transit
- Strong encryption, but ignoring security warnings
  - Ignoring certificate validation errors
  - Falling back to plain text after failures

**Impact**

- Man-in-the-middle attacks
- Tampering w/ data in transit
- Confidentiality of data lost
M3- Insufficient Transport Layer Protection

Prevention Tips

- Ensure that all sensitive data leaving the device is encrypted
- This includes data over carrier networks, WiFi, and even NFC
- When security exceptions are thrown, it’s generally for a reason… *DO NOT* ignore them!

<table>
<thead>
<tr>
<th>Control#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.3.6</td>
<td>Ensure sensitive data is protected in transit</td>
</tr>
</tbody>
</table>
M4- Client Side Injection

- **Apps using browser libraries**
  - Pure web apps
  - Hybrid web/native apps

- **Some familiar faces**
  - XSS and HTML Injection
  - SQL Injection

- **New and exciting twists**
  - Abusing phone dialer + SMS
  - Abusing in-app payments

**Impact**
- Device compromise
- Toll fraud
- Privilege escalation
M4- Client Side Injection

**Prevention Tips**

- Sanitize or escape untrusted data before rendering or executing it
- Use prepared statements for database calls…concatenation is still bad, and always will be bad
- Minimize the sensitive native capabilities tied to hybrid web functionality

<table>
<thead>
<tr>
<th>Control#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>Pay particular attention to validating all data received from and sent to non-trusted third party apps before processing</td>
</tr>
<tr>
<td>10.1-10.5</td>
<td>Carefully check any runtime interpretation of code for errors</td>
</tr>
</tbody>
</table>
M5- Poor Authorization and Authentication

- Part mobile, part architecture
- Some apps rely solely on immutable, potentially compromised values (IMEI, IMSI, UUID)
- Hardware identifiers persist across data wipes and factory resets
- Adding contextual information is useful, but not foolproof

**Impact**

- Privilege escalation
- Unauthorized access
M5- Poor Authorization and Authentication  

Prevention Tips

- Contextual info can enhance things, but only as part of a multi-factor implementation
- Out-of-band doesn’t work when it’s all the same device
- Never use device ID or subscriber ID as sole authenticator

<table>
<thead>
<tr>
<th>Control#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1-4.6</td>
<td>Implement user authentication/authorization and session management correctly</td>
</tr>
<tr>
<td>8.4</td>
<td>Authenticate all API calls to paid resources</td>
</tr>
</tbody>
</table>
M6- Improper Session Handling

- Mobile app sessions are generally MUCH longer
- Why? Convenience and usability
- Apps maintain sessions via
  - HTTP cookies
  - OAuth tokens
  - SSO authentication services
- Bad idea= using a device identifier as a session token

Impact
- Privilege escalation
- Unauthorized access
- Circumvent licensing and payments
M6- Improper Session Handling

Prevention Tips

- Don’t be afraid to make users re-authenticate every so often
- Ensure that tokens can be revoked quickly in the event of a lost/stolen device
- Utilize high entropy, tested token generation resources

<table>
<thead>
<tr>
<th>Control#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.13</td>
<td>Use non-persistent identifiers</td>
</tr>
<tr>
<td>4.1-4.6</td>
<td>Implement user authentication/authorization and session management correctly</td>
</tr>
</tbody>
</table>
M7- Security Decisions Via Untrusted Inputs

• Can be leveraged to bypass permissions and security models
• Similar but different depending on platform
  - iOS- Abusing URL Schemes
  - Android- Abusing Intents
• Several attack vectors
  - Malicious apps
  - Client side injection

Impact
• Consuming paid resources
• Data exfiltration
• Privilege escalation
M7- Security Decisions Via Untrusted Inputs

Prevention Tips

- Check caller’s permissions at input boundaries
- Prompt the user for additional authorization before allowing
- Where permission checks cannot be performed, ensure additional steps required to launch sensitive actions

<table>
<thead>
<tr>
<th>Control#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2</td>
<td>Run interpreters at minimal privilege levels</td>
</tr>
</tbody>
</table>
M8- Side Channel Data Leakage

- Mix of not disabling platform features and programmatic flaws
- Sensitive data ends up in unintended places
  - Web caches
  - Keystroke logging
  - Screenshots (ie- iOS backgrounding)
  - Logs (system, crash)
  - Temp directories
- Understand what 3rd party libraries in your apps are doing with user data (ie- ad networks, analytics)

Impact

- Data retained indefinitely
- Privacy violations
M8- Side Channel Data Leakage

Prevention Tips

- Never log credentials, PII, or other sensitive data to system logs
- Remove sensitive data before screenshots are taken, disable keystroke logging per field, and utilize anti-caching directives for web content
- Debug your apps before releasing them to observe files created, written to, or modified in any way
- Carefully review any third party libraries you introduce and the data they consume
- Test your applications across as many platform versions as possible

<table>
<thead>
<tr>
<th>Control#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.3</td>
<td>Check whether you are collecting PII, it may not always be obvious</td>
</tr>
<tr>
<td>7.4</td>
<td>Audit communication mechanisms to check for unintended leaks (e.g. image metadata)</td>
</tr>
</tbody>
</table>
M9- Broken Cryptography

- Two primary categories
  - Broken implementations using strong crypto libraries
  - Custom, easily defeated crypto implementations
- Encoding != encryption
- Obfuscation != encryption
- Serialization != encryption

Impact

- Confidentiality of data lost
- Privilege escalation
- Circumvent business logic
M9- Broken Cryptography

*Prevention Tips*

- Storing the key with the encrypted data negates everything
- Leverage battle-tested crypto libraries vice writing your own
- Take advantage of what your platform already provides!

<table>
<thead>
<tr>
<th>Control#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3</td>
<td>Utilize file encryption API’s</td>
</tr>
<tr>
<td>2.3</td>
<td>Leverage secure containers</td>
</tr>
</tbody>
</table>
M10- Sensitive Information Disclosure

- We differentiate by stored (M1) vs. embedded/hardcoded (M10)
- Apps can be reverse engineered with relative ease
- Code obfuscation raises the bar, but doesn’t eliminate the risk
- Commonly found “treasures”:
  - API keys
  - Passwords
  - Sensitive business logic

Impact

- Credentials disclosed
- Intellectual property exposed
M10- Sensitive Information Disclosure

Prevention Tips

- Private API keys are called that for a reason…keep them off of the client
- Keep proprietary and sensitive business logic on the server
- Almost never a legitimate reason to hardcode a password (if there is, you have other problems)

<table>
<thead>
<tr>
<th>Control#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.10</td>
<td>Do not store any passwords or secrets in the application binary</td>
</tr>
</tbody>
</table>
Conclusion
Mobile Money Service Provider Challenge: “Balance”
Thank you!!!
AT THE SPEED OF IDEAS™