SoftwareGroup
doing it right

Technology and Alternative Delivery Channels

Asia Pacific Financial Inclusion Summit

Charlene Bachman

29 October 2015

SoftwareGroup
doing it right

Introduction

Workshop objective:

1. Introduce the ADC technology handbook
2. Present an overview of the content
3. Review ADC options and trends
4. Technology Implementation Process Explained

SoftwareGroup
doing it right

Introduction

The ambition to acieve financial inclusion requires that we address the challenge of delivering appropriate and affordable financial services to an estimated 2 billion unbanked individuals globally.

2014 Global Findex reports the world's "unbanked" population shrank by 20 % to 2 billion adults between 2011 and 2014 as 700 million gained access to financial services.

SoftwareGroup
doing it right

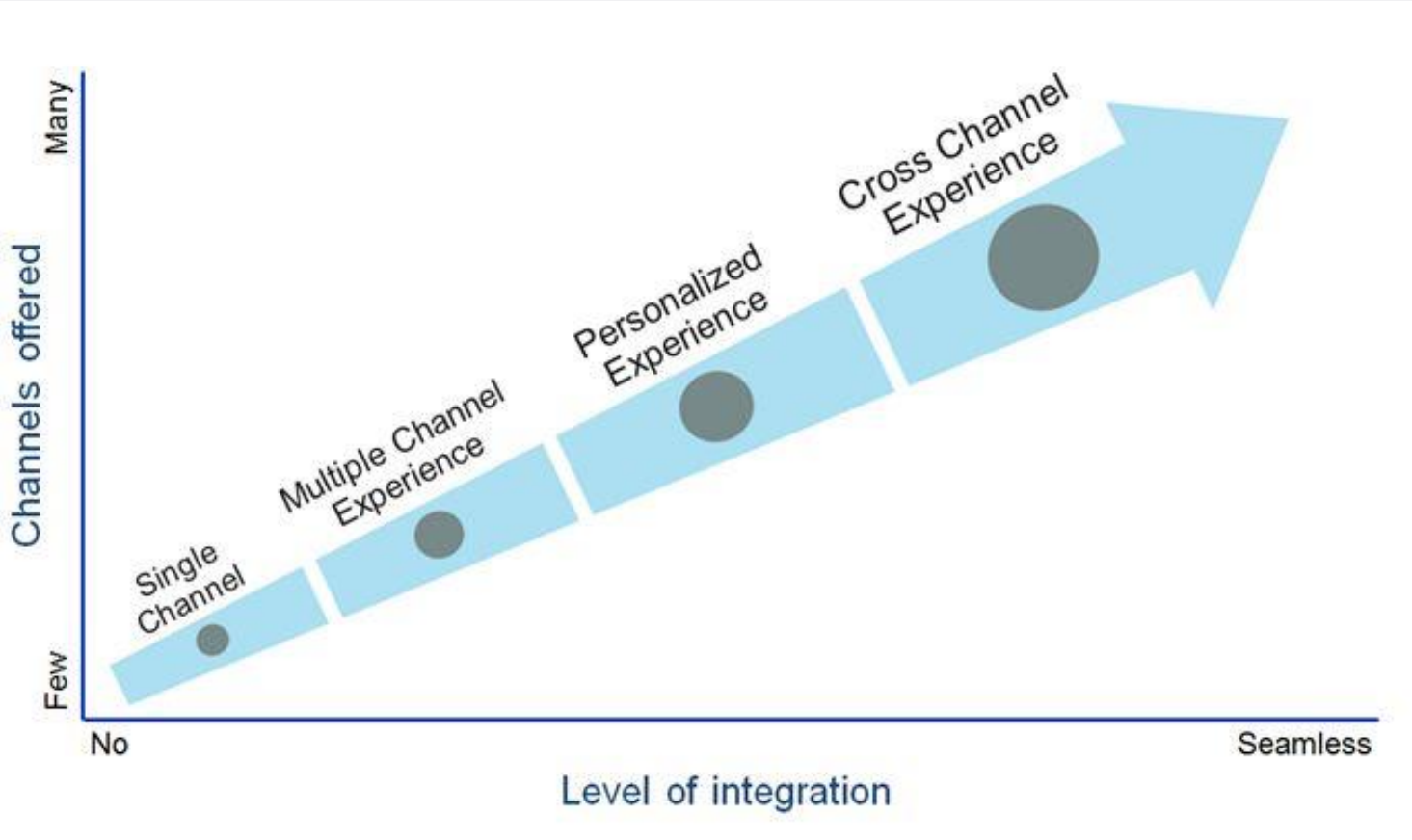
Look Familiar?

SoftwareGroup
doing it right

Alternative Delivery Channels

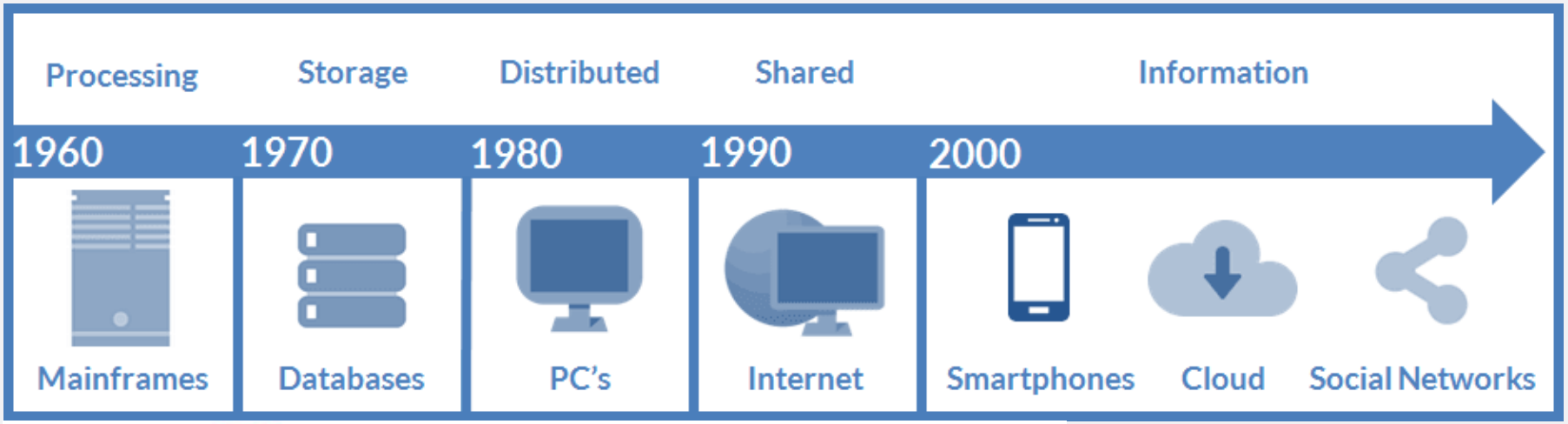
Channels that expand the reach of services beyond the traditional bank branch channel.

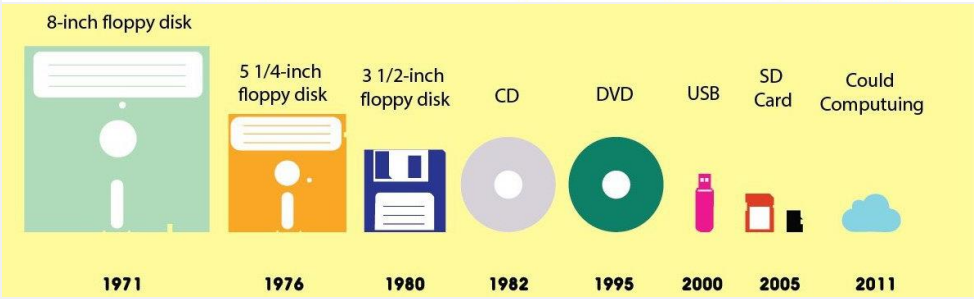
Customers want access Anytime, Anywhere, Anyhow



Source: Meeting customer expectations with an excellent multi-channel service delivery Accenture

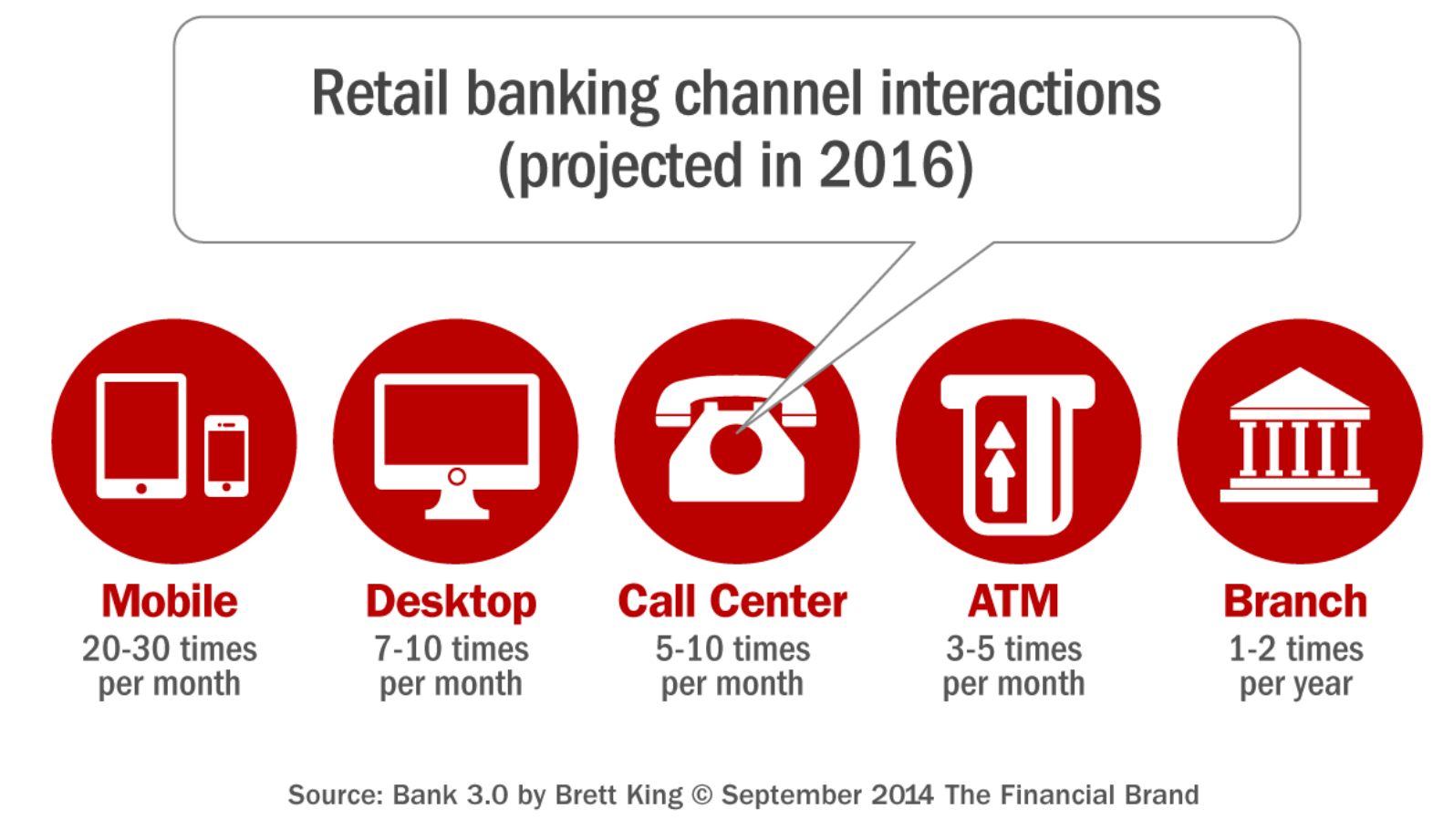
Evolution of Technology





SoftwareGroup
doing it right

Demand for Digital Access

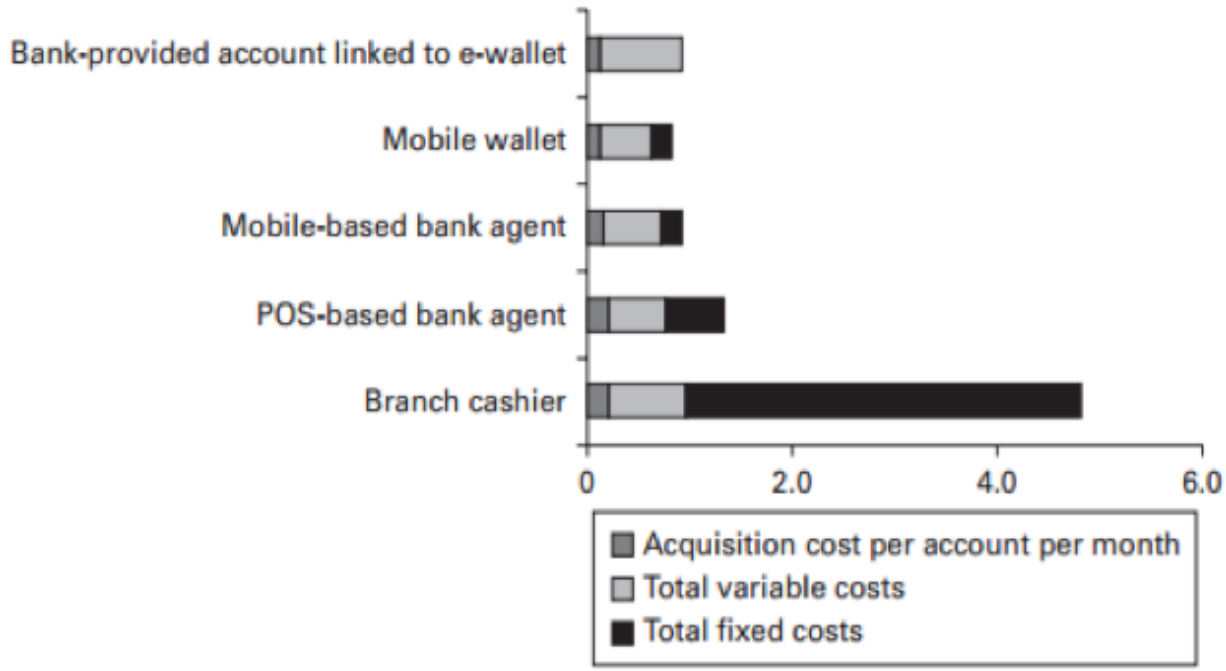


SoftwareGroup
doing it right

Driven by costs, expansion, efficiency + innovation

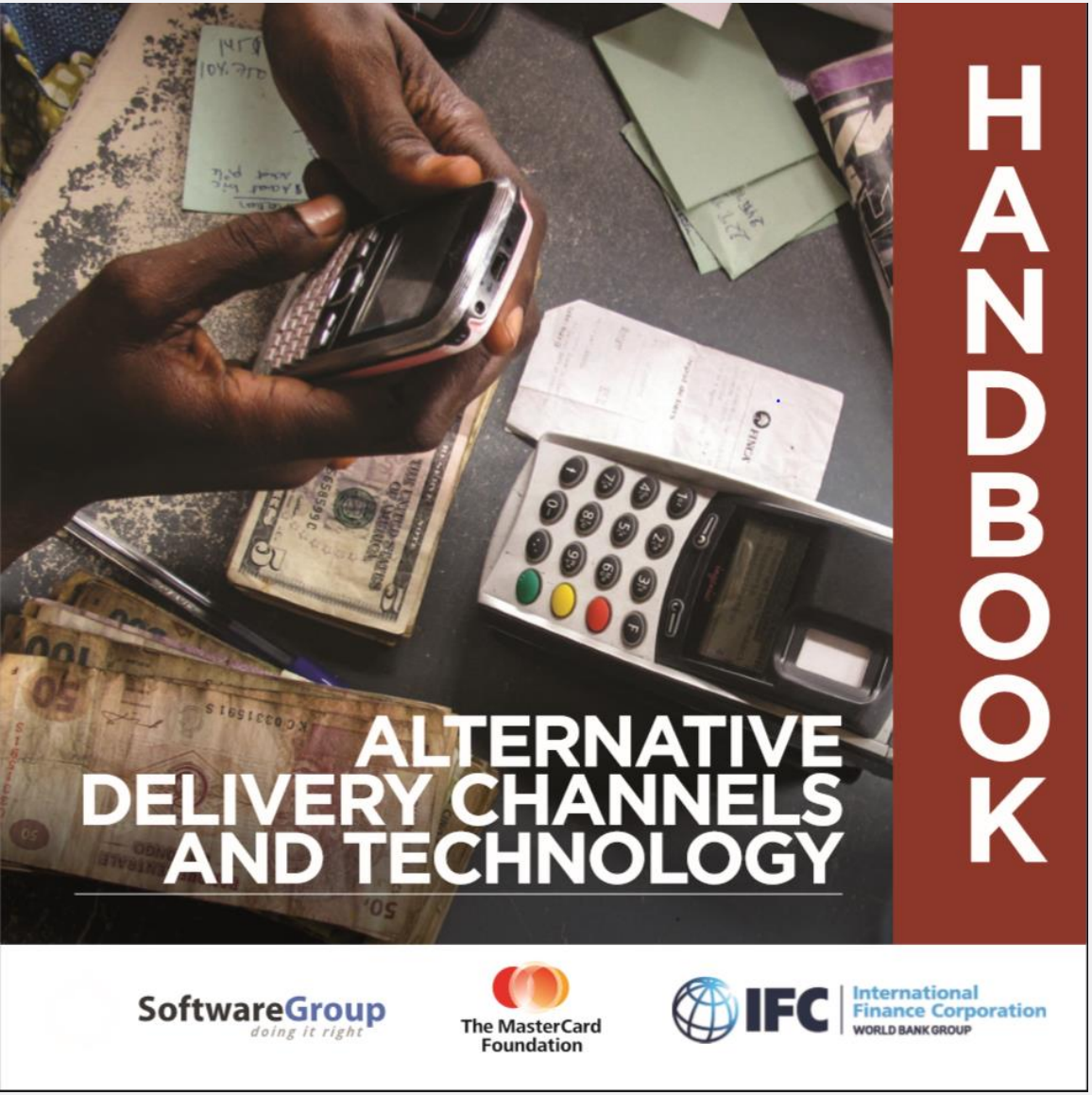
The cost of servicing an account over the various channels differs drastically showing again how the branch is the most expensive ($5/month/account) vs less than $2 for mobile based agents or mobile accounts.

Figure 12.2 Monthly Costs in Dollars Associated with an Illustrative Transaction Account



Innovation is introducing new players and business models, pushing retail banks towards ADCs

ADC & Technology Handbook



This handbook serves as a tool for FSPs to increase the technical understanding of ADCs and technology platforms and to provide practical guidance on how to approach an ADC technology project.

SoftwareGroup
doing it right

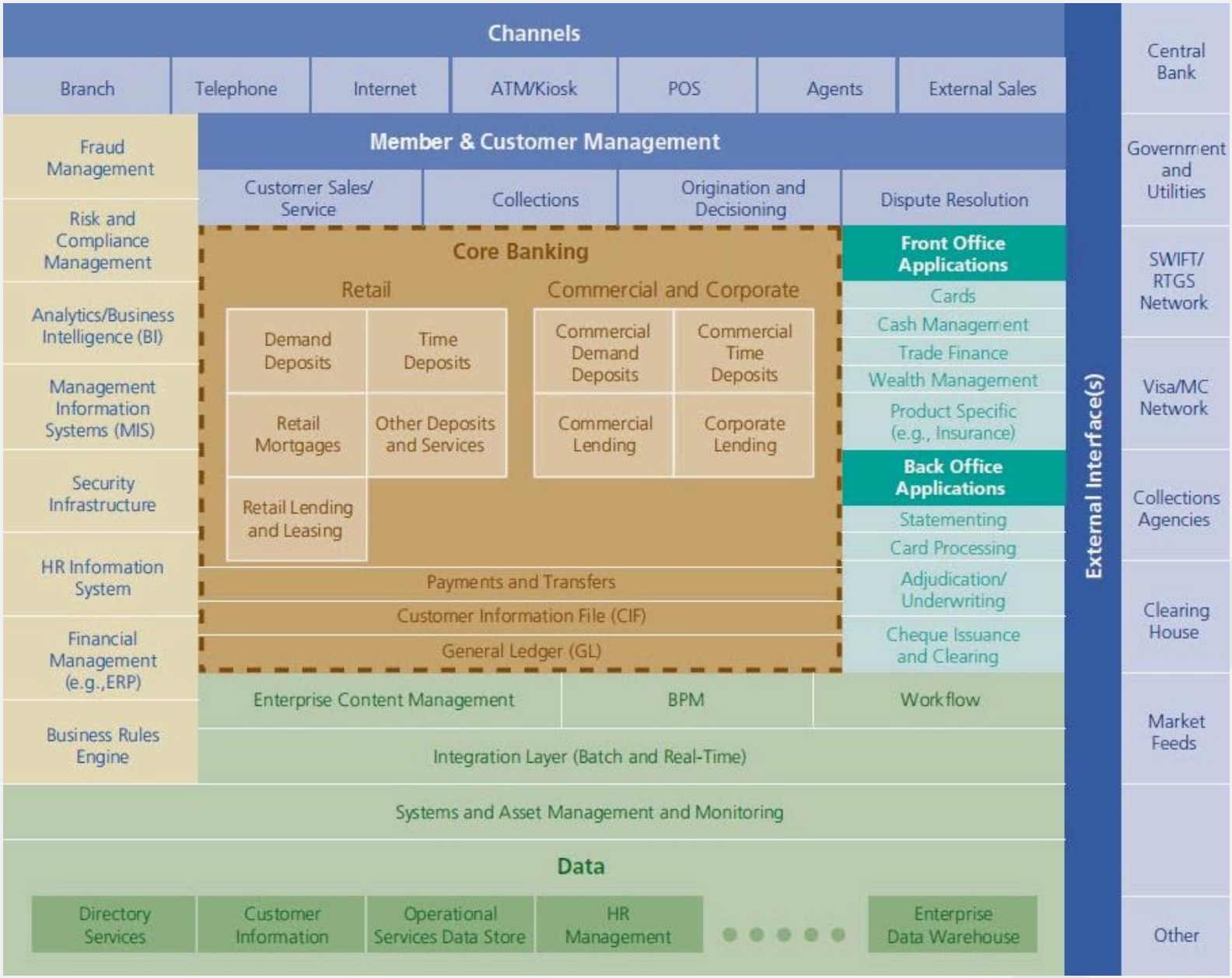
ADC Terminology

Term	Definition
Channel	The customers access point to the FI, namely who or what the customer interacts with to access financial services. One channel has multiple technology options: agency works on mobile, web or POS
Enabling Technology	The underlying technology platform used to drive the channel ie POS, Mobile, ATM. This technology consists of a hardware device, a software application and a means of connectivity/communication
Self Service Channel	A channel that is available to customers without any other human interaction- ie don't need an agent or FI staff invovled eg Internet Banking, Mobile Banking and Self Service Terminals
Over the Counter Channel	A channel that requires the customer to interact with either a staff member or third party (agent, merchant) to transact. eg. Agency banking, Extension services

ADC Technology Implementation Process

SoftwareGroup
doing it right

Comprehensive Technology Architecture

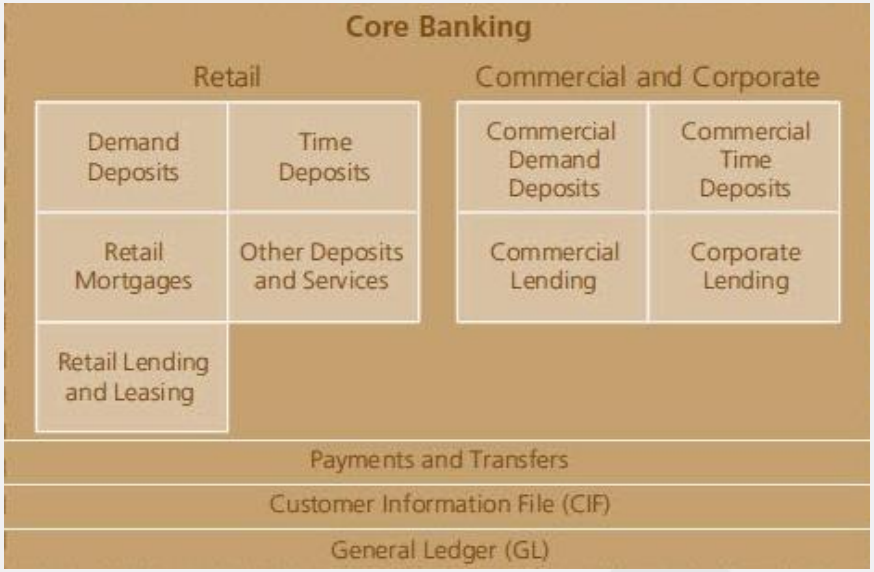


SoftwareGroup
doing it right

Overview: Core Banking System

What is it? The core system that supports a bank's most common transactions. Includes definition of products/services, account opening/maintenance, loan workflow/tracking, teller services, customer management etc. For many FI's this is the most critical system for their operations.

Why it's needed? Necessary unless you want to use pen/paper or Excel! Provides the logic/algorithm for products and system based controls for all operations related to the customer.



Examples:

Infosys Finacle | Craft Silicon Thinking. Crafting. Transforming. | neptune Neptune Software Group | TEMENOS The Banking Software Company | MAMBU | Mifos

SoftwareGroup doing it right

ADC's: Business Perspective

	CHANNEL NAME	TYPE OF CHANNEL	WHO/WHAT CUSTOMER INTERACTS WITH TO TRANSACT	SAMPLE FUNCTIONALITY OFFERED BY THE CHANEL
	ATM	*Self-service*	*ATM*	*Cash out, balance enquiry, payments, cash deposit*
	Internet banking	*Self-service*	*Computer, phone, tablet, kiosk*	*Enquiries, transfers, payments*
	Agent banking	*OTC*	*3rd party agent, merchant, phone, POS, mobile*	*Cash in, cash out, payments*
	Extension services, (field staff, mini branch, branch on wheels)	*OTC*	*Bank staff: loan officer, susu collector, other FSP staff, POS, mobile*	*Account opening, cash in, cash out, loan applications, enquiries*
	Mobile banking	*Self-service*	*Phone*	*Enquiries, transfers, payments*
	E-wallet (m-wallets, prepaid cards, store cards)	*Self-service + OTC*	*Phone, computer, merchant, kiosk, ATM, agent, card*	*Cash in, cash out, payments, transfers*
	Call center	*OTC*	*Phone, customer service rep*	*Enquiries, transfers, payments*

Most commonly used channels.

How to use the channel?

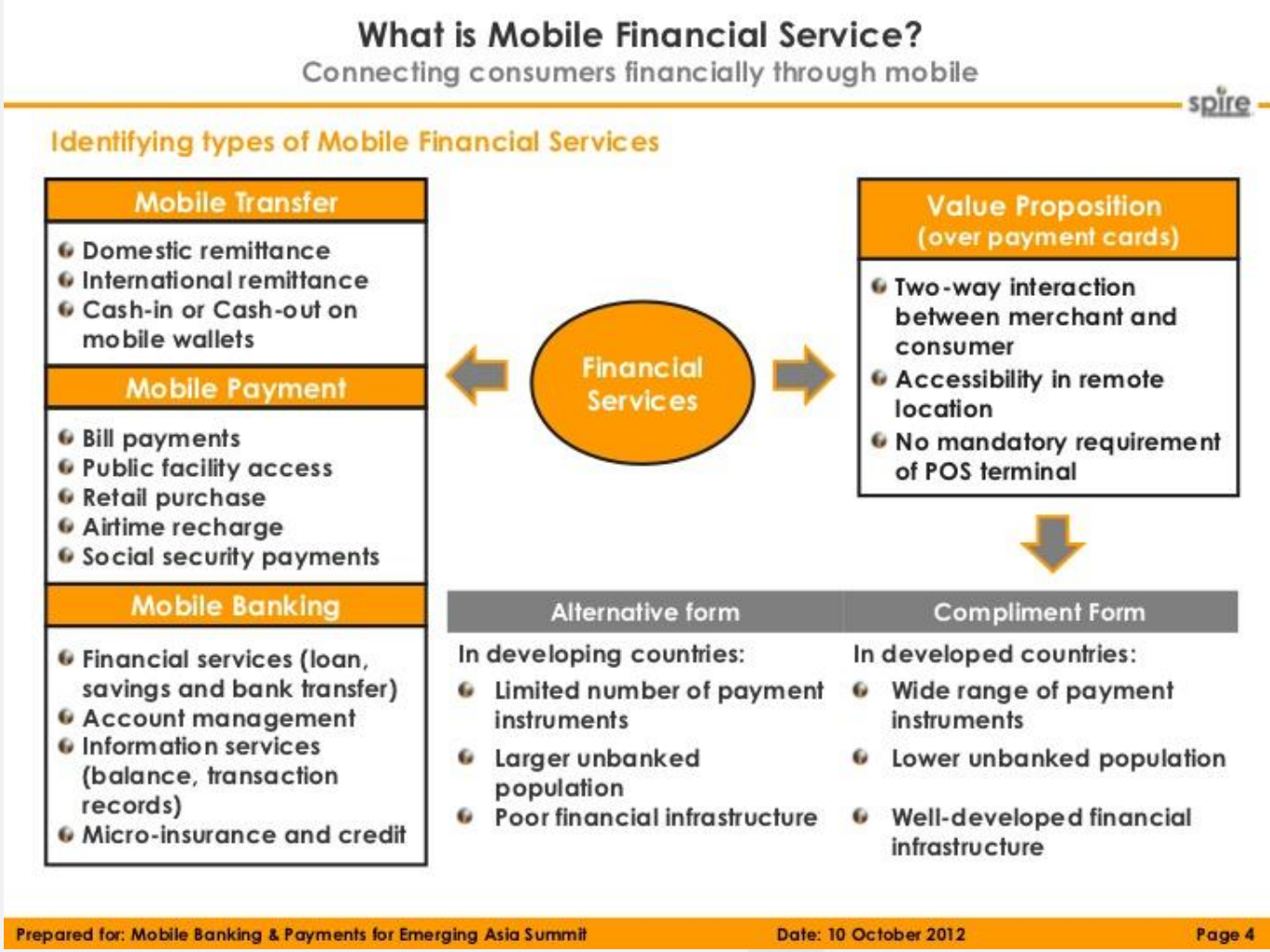
Who is the user?

SoftwareGroup
doing it right

ADC's: Available Options

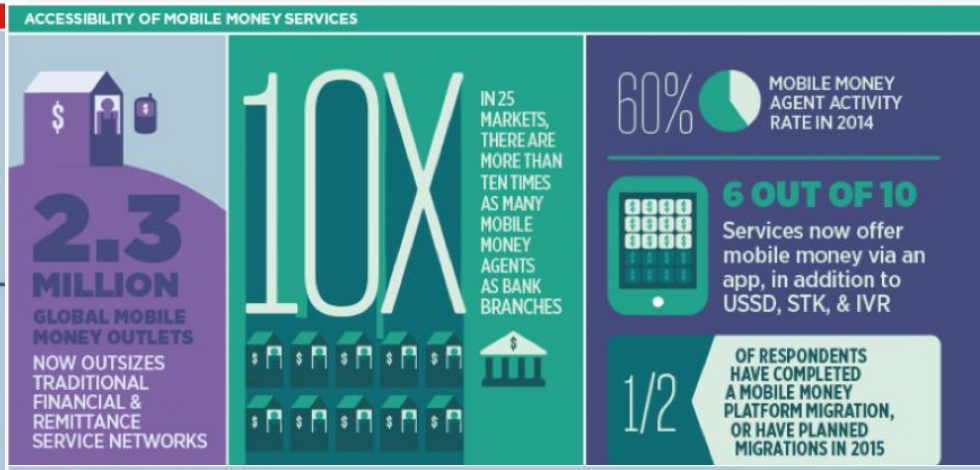
Mobile Financial Services Overview

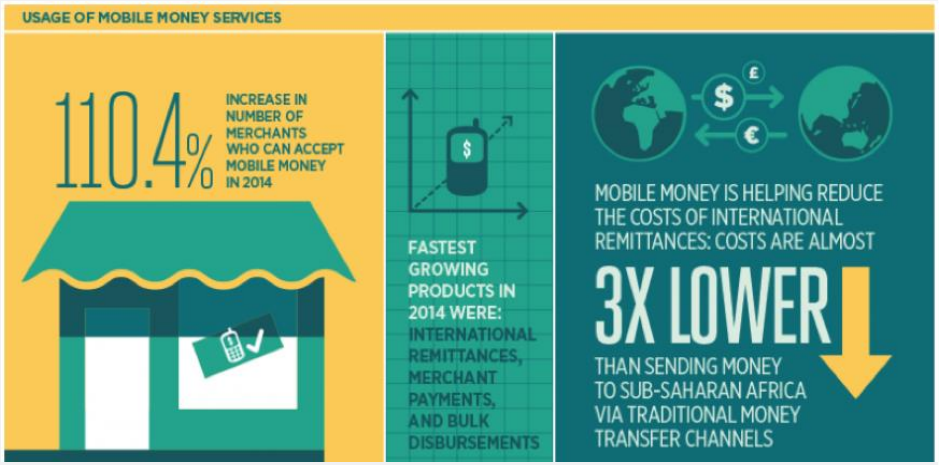
Within ADCs, those that rely on the use of a mobile phone are collectively called Mobile Financial Services (MFS). These are radically changing the financial inclusion space, particularly through us of mobile money. We will look at each MFS channel separately: **Mobile Money, Mobile Banking, Agency, Extension Services** and **Merchant Services**.



SoftwareGroup

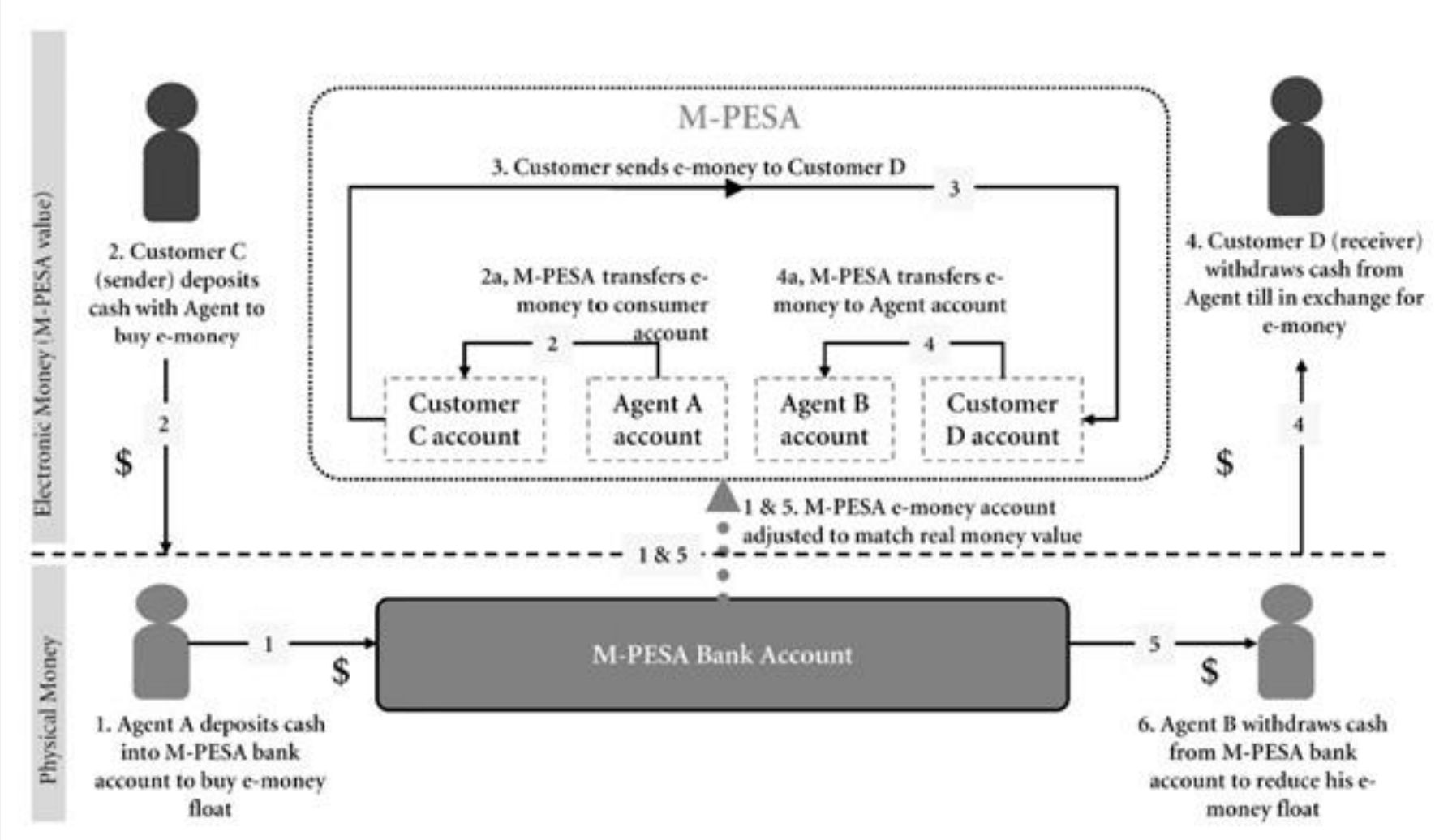
MFS: Mobile Money





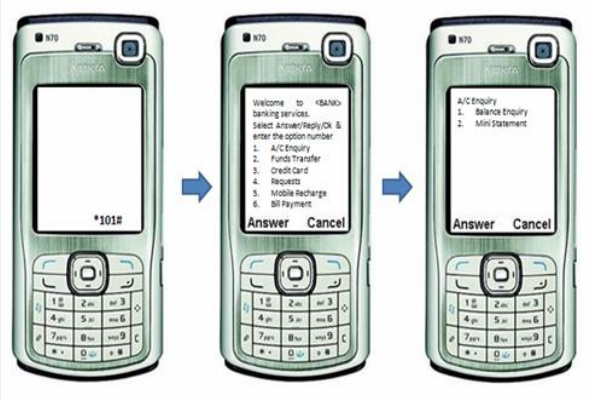
SoftwareGroup
doing it right

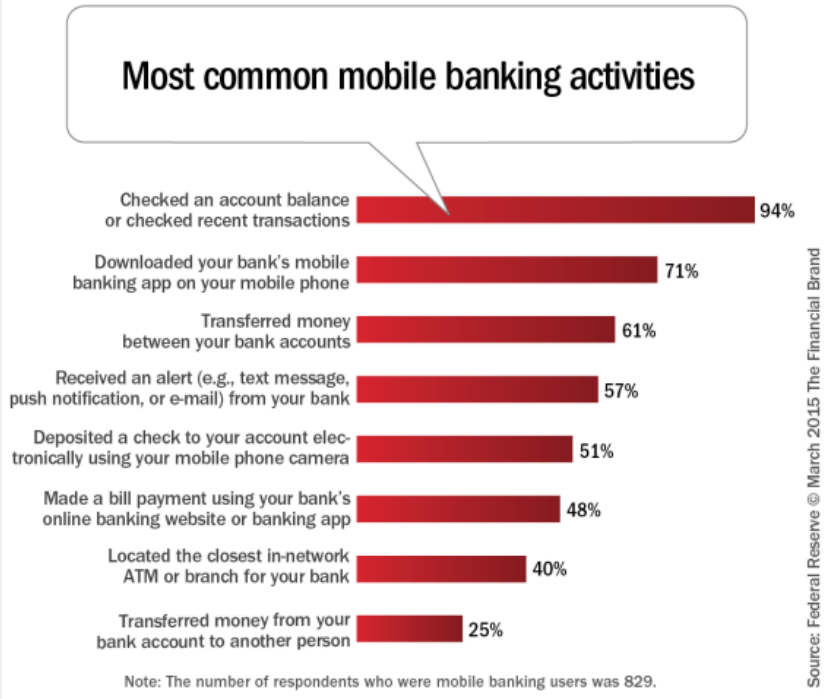
MFS: Mobile Money - Mwallet



MFS: Mobile Banking

The use of a mobile phone by a consumer/client to access financial services (financial and non financial transactions). The account being accessed is a full bank account rather than a virtual e-money account. However, it is very common to have a linkage between this service and the m-wallet to enable bank to wallet transfers.





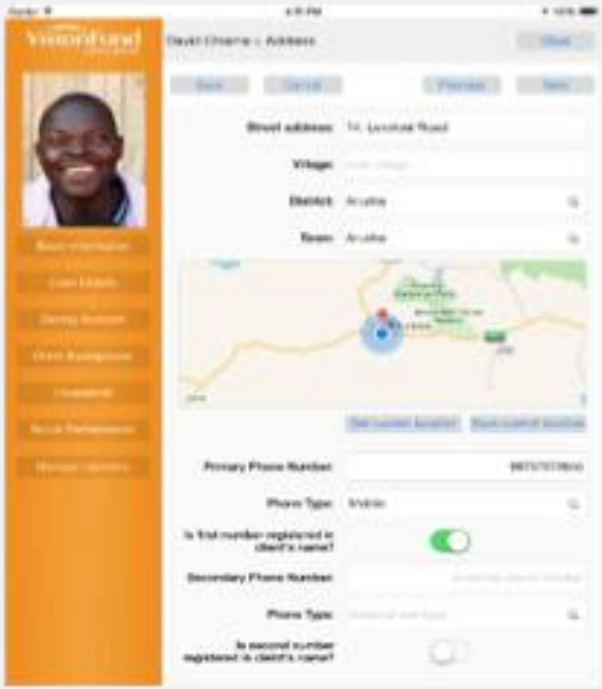
SoftwareGroup
doing it right

MFS: Agency Banking

Banking services offered by a third party agent who is authorised by the bank to provide limited services to clients, typically cash in/out. Note that mobile money also requires an agent network to support cash in/out to wallets but in this case the network is managed by the mobile money provider. Different technology options are available for agency including: POS, mobile or web portal.

MFS : Extension Services/Digital Field Applications

Use of a mobile device (phone, tablet or POS) by staff of the FI to provide services outside of the branch. This could be used only for non financial services such as customer registration, account opening, loan applications or could support financial transactions such as deposits, group collection sheets and even withdrawals.



SoftwareGroup
doing it right

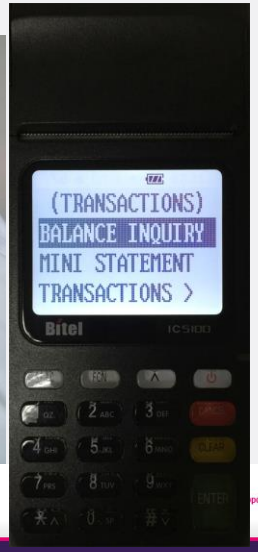
MFS : Mobile Merchant Services

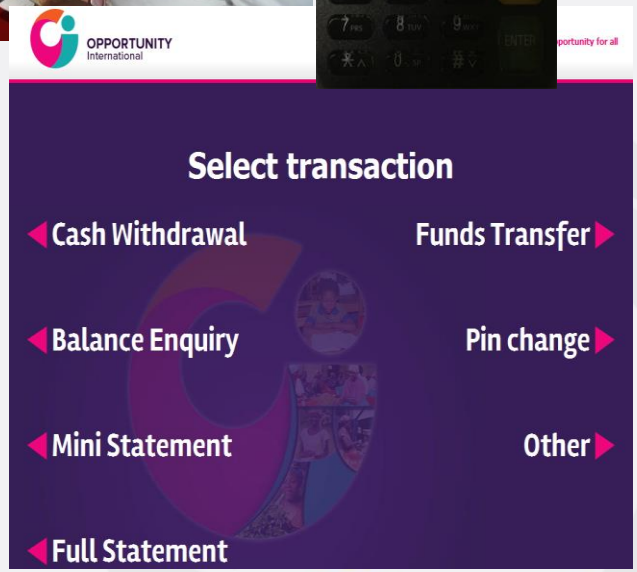
Merchant payments which have traditionally relied on use of a physical POS device and a payment card are now moving to embrace mobile technology. This can either be in the form of an m-POS as a replacement of the physical POS or could use either mobile banking or mobile wallets to make a payment directly to the merchant account, without the use of a payment card.

SoftwareGroup
doing it right

ADC: ATM & POS Network Management

Device management and monitoring tools to manage a network of ATMs and/or POS devices. Fully integrated with HSM and Card Management for full service operations of electronic banking channel. Monitoring screens display the status of all devices.





Business Case

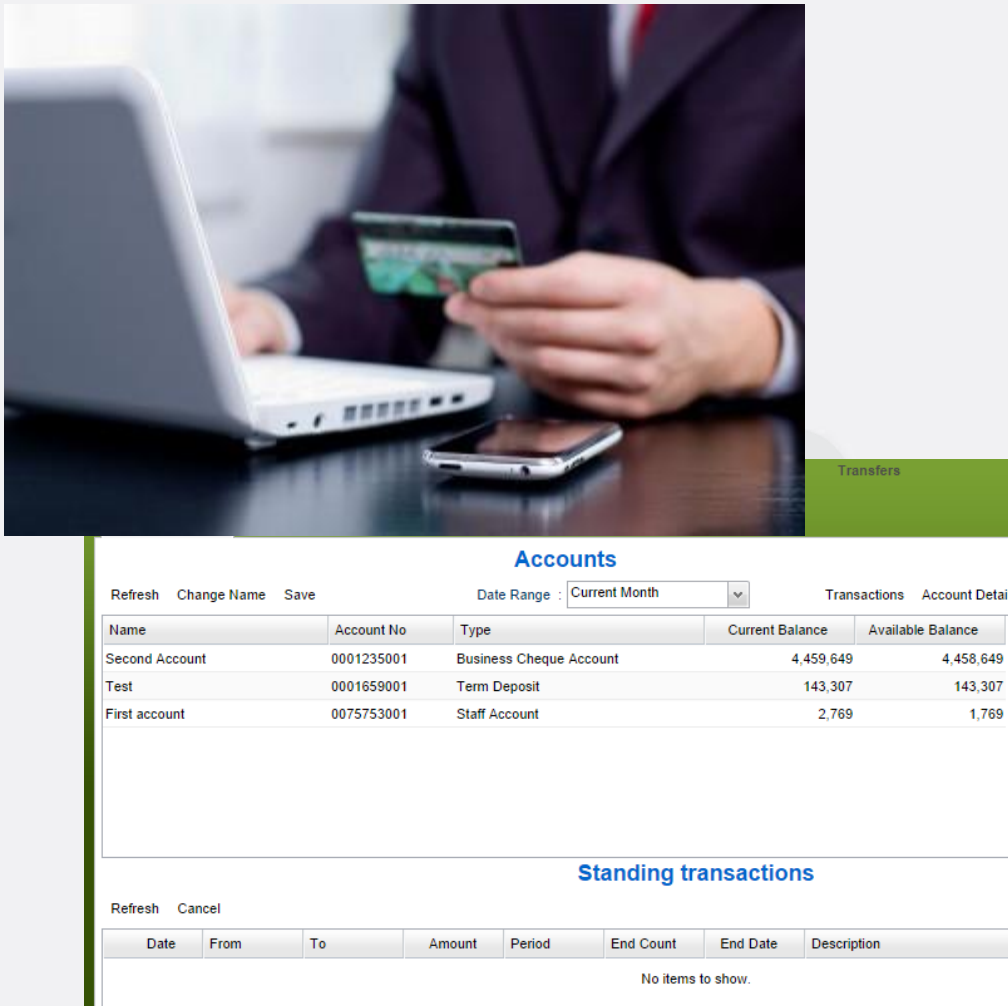
- Expand the reach of services with secure and automated devices
- Manage a proprietary network of ATM to offer 24/7 banking
- Leverage “on-us” ATM network to avoid third party fees for clients
- Customise client interaction according to workflow requirements
- Distribute POS devices to retailer for more convenient payments

Internet Banking

Web portal that provides clients convenient self-service access to their accounts and services, both retail and corporate. Clients can update their user profile, transact, access statements, manage payees, and schedule payments via a user-friendly interface.

Business Case

- Allow customers to access their information 24/7
- Improve convenience with online account opening and applications
- Increase transaction volume with self-service transactions and bill pay
- Supports different user groups and rights for corporate banking.
- CBS independent

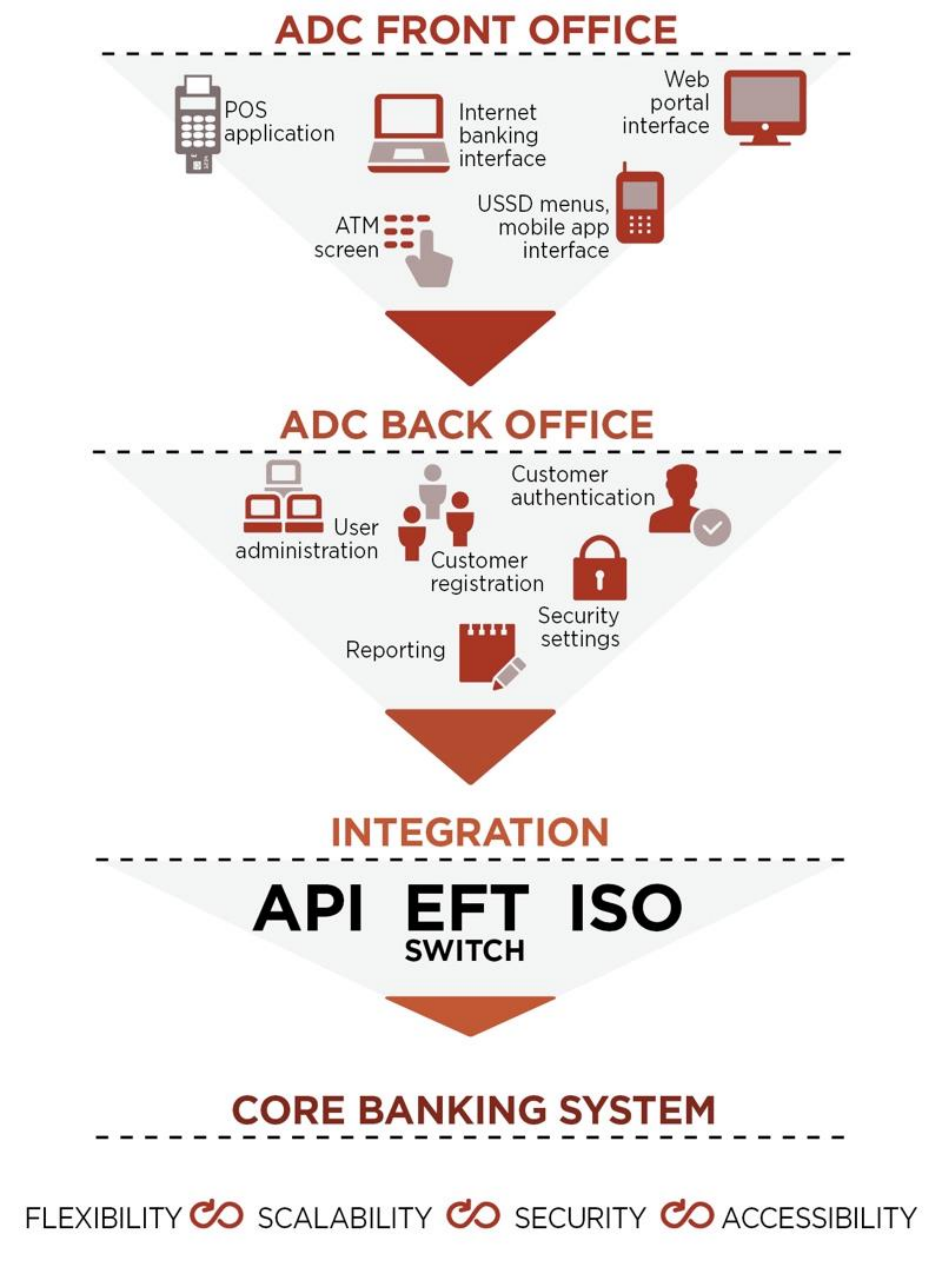


ADC's: Technology Perspective

	CHANNEL NAME	DEVICE	APPLICATION	COMMUNICATION	AUTHENTICITY MODE
	ATM	*ATM, HSM*	*Bespoke tech*	*LAN (physical leased line, P2P satellite, VPN over internet, wireless), modem (GPRS, dial-up)*	*Card / PIN, bio, mobile*
	Internet banking	*Computer, phone, tablet, kiosk*	*Web*	*Internet (mobile, wireless, leased line)*	*Username, password, OTP*
	Agent / merchant	*Computer, phone, tablet, POS*	*Web, POS, mobile*	*Internet (mobile, wireless, leased line), mobile data (GPRS, 3G, 4G)*	*PIN, card, bio, physical ID*
	Extension services, (field staff, mini branch, branch on wheels)	*Computer, phone, tablet, POS*	*Web, POS, mobile*	*Internet (mobile, wireless, leased line), mobile data (GPRS, 3G, 4G)*	*PIN, card, bio, physical ID*
	Mobile banking	*Phone*	*Mobile*	*Mobile data (GPRS, 3G, 4G), SMPP, USSD*	*PIN, OTP*
	E-wallet (m-wallets, prepaid cards, store cards)	*Phone, computer, kiosk, ATM, POS*	*Web, POS, mobile, bespoke tech (ATM)*	*Internet (mobile, wireless, leased line), mobile data (GPRS, 3G, 4G)*	*PIN, card, physical ID*
	Call center	*Phone*	*IVR*	*Telecoms – Voice*	*Password*

SoftwareGroup
doing it right

Channel Architecture



A channel solution has 4 components all of which must be considered during requirements analysis and selection:

1. A physical device
2. An application running on the device
3. A communication channel used to exchange data between the device and the FSP's host system
4. An authentication mode used to confirm the identity of the user of the channel.

ADC Front Office Options: Applications

ADC applications The application layer of ADC solutions consists of front-end applications, backoffice administration modules, and the integrations between these systems and the Core Banking System

APPLICATION OPTION	ADVANTAGES	DISADVANTAGES
SMS	• *Available in all countries and relatively easy to set up.* • *Accessible on all handsets.* • *Lower dependency on relationship between the MNO and the FSP (can send to all networks unlike USSD, which is per network).* • *Easy to use and most customers familiar with the technology.*	• *Very limited functionality due to limit of message size and non-real-time connection.* • *Limited security, as data entered in SMS is available as clear text in sent messages.* • *Delay in delivery of messages can occur and is beyond control of the FSP.*
STK	• *No software installation required.* • *Device independent, so will work on all handsets.* • *User-friendly menu interface.* • *Encryption keys are stored on the SIM, so applications have control over the security levels.* • *If FSP has access to STK, they can have full control over the channel – (less dependent on third party).*	• *Requires MNO or MVNO license.* • *Involves issuing of SIM cards.* • *Updates to the application are difficult to coordinate, requiring either reissue of SIMs or Over the Air push updates.* • *Customers may need to manage a 2nd SIM card (though not necessarily replace their network SIM) or apply a skin SIM.*
USSD	• *No software installation required.* • *Device independent, so will work on all handsets.* • *User-friendly menu interface.* • *Encryption is in-built in channel, providing good security.* • *No information is recorded on the device.* • *Usage is tied to a registered phone number, which aids in the authentication process of the user.*	• *Not available in all countries.* • *Requires an agreement with an MNO, which is not always forthcoming.* • *No support for peripherals, such as card readers, biometrics, or receipt printers.* • *Primarily supports financial transactions.* • *Limited session length.* • *No offline support.* • *Can be more costly than others depending on MNO communication fees (which are often beyond the control of the FSP to influence).* • *Security (encryption) is fully dependent on the provider of the channel.* • *In many countries, the frequency of dropped sessions is high and still charged to the customer, regardless of whether a transaction was completed successfully.*

ftwareGroup
doing it right

ADC Front Office Options: Applications

APPLICATION OPTION	ADVANTAGES	DISADVANTAGES
NATIVE MOBILE APPS	• *User-friendly and rich user interface.* • *More functionality available – camera, signature, and GPS.* • *Supports connections to peripherals: bio devices, card readers, and Bluetooth printers.* • *Can work offline/online and even in online mode can be more forgiving of poor quality connections.* • *Suited to both financial and non-financial transactions.*	• *Manual intervention required to install and updates often required.* • *Requires support for specific or multiple devices/operating systems, so different versions are required (Java, Android, or iOS).* • *Security must be built in and is not automatically present.* • *Multiple functionalities typically require use of external devices.* • *Compatible handsets tend to be more expensive (feature phone or smartphone), hence less accessible to the full market.*
WEB APPS	• *No software installation required.* • *User-friendly and rich user interface.* • *Full functionality available, but limited access to peripherals.* • *Can be used on different devices (mobile/tablet/netbooks/notebooks).* • *Suited to both financial and non-financial transactions.*	• *Requires good continuous data connectivity.* • *No offline support.* • *Security must be built in and is not automatically present.* • *Requires support of multiple browsers.* • *Limited access to peripherals.* • *Compatible handsets tend to be more expensive (feature phone or smartphone), hence less accessible to the full market.*
WEB PORTAL	• *Can use CBS directly if a Web-based system is available.* • *No software installation required.* • *User-friendly and rich user interface.* • *Full functionality available, but limited access to peripherals.* • *Can be used on different devices (mobile/tablet/netbooks/notebooks), with some limitations.*	• *Requires a reliable and continuous data connection to use (no offline support).* • *Limited access to peripherals (Bluetooth printers and card readers).* • *When used on a tablet/smartphone, usability may not be as good as a mobile application.*
IVR	• *Ability to serve large numbers of customers simultaneously.* • *Pre-recorded messages for consistent accurate communication of information.* • *Limited human intervention to maintain – enables customers to do their own transactions without having to talk with someone.* • *Hosted solutions for small institutions with limited technology experience.*	• *Speech recognition makes it more difficult to navigate an IVR and customers will be inclined to speak with a live person.* • *Complicated menu levels and choices; it can be easy to get lost in IVR.* • *Cost of hosting can be high, depending on the usage.*

SoftwareGroup
doing it right

ADC Front Office Options: Devices

The physical object with which a user interacts, such as a mobile phone or ATM

DEVICE OPTION	ADVANTAGES	DISADVANTAGES
BASIC PHONE	• *Cheapest handset/device available.*	• *Only compatible with USSD and STK applications.*
FEATURE PHONE	• *Still relatively low cost compared with other options.* • *Good battery life (compared to smartphones).* • *Flexible in many ways: operation types, peripherals, multi-purpose.* • *Good usability if used for small amounts of data.* • *Excellent portability.* • *Embedded data transfer/GPS capabilities.*	• *More expensive than basic phones.* • *Phone features may limit its function and usability (GPS, Bluetooth, touch screen – model dependent).* • *Peripheral functionality is managed on separate devices (bio reader and printers) and not in-built as with a POS.* • *Less popular platform for app development so may have less access to other apps (if required).* • *Peripherals are limited and need to be managed separately.* • *Not suited to entry of large amounts of data.* • *No in-built security.*
SMARTPHONE	• *Moderate hardware cost relative to processing capacity.* • *Flexible in many ways: operation types, peripherals, multi-purpose.* • *Good usability if used for small to moderate amounts of data.* • *Excellent portability.* • *Embedded data transfer/GPS capabilities.* • *Access to a wide variety of apps/popular development platform.*	• *Peripheral functionality is managed on separate devices (i.e. bio reader, printers) and not in-built as with a POS* • *Battery life may limit some uses (Bluetooth and GPS).* • *Not suited to entry of large amounts of data.* • *No in-built security, but can be added as peripherals or embedded in app.* • *More expensive option compared with feature/basic phones.*

ADC Front Office Options: Devices

DEVICE OPTION	ADVANTAGES	DISADVANTAGES
TABLET	• *Flexible in many ways: operation types, peripherals, multi-purpose.* • *Good usability – including more comprehensive screens – reports, and data entry.* • *Good portability.* • *Good battery life for specific models.* • *Embedded data transfer/GPS capabilities.* • *Access to wide variety of apps/popular development platform.*	• *Peripherals need to be managed separately, although some accessories such as tablet covers are available with biometric reader and card scanner built in.* • *Battery life may limit some uses (Bluetooth and GPS).* • *No in-built security, but can be added as peripherals or imbedded in app.* • *Relatively expensive option, although some low-cost options exist.*
LAPTOP/ NETBOOK	• *Flexible in many ways: operation types, peripherals, multi-purpose.* • *Excellent usability.* • *Longest battery life for specific models.* • *Can potentially extend the use: access Web-based CBS and other systems directly.* • *Significant computational power compared with mobile devices.*	• *Requires more training/support and computer literacy.* • *Less portable.* • *Potentially less battery life.* • *No in-built security, but can be added as peripherals.* • *Most expensive device option.*
POS (DEVICE + APP)	• *Strong in-built security.* • *Device is portable and durable.* • *Single device for multiple functions (bio, print, card reader, SIM card) which is a must for many agent banking platforms that require receipts.* • *Fast operation.* • *Limited misuse.*	• *Restricted functionality due to numeric keypad (mostly suitable for financial transactions).* • *Specialized training required for users to operate and troubleshoot the devices/application.* • *Installation and updates support is required often, with some level of manual intervention.* • *Communication capabilities are optional and influence the price (SIM card versus cable or Wi-Fi).* • *Limited offline capabilities.* • *Limited vendors/developers and often have restricted access to device.* • *Cost of device.*

SoftwareGroup
doing it right

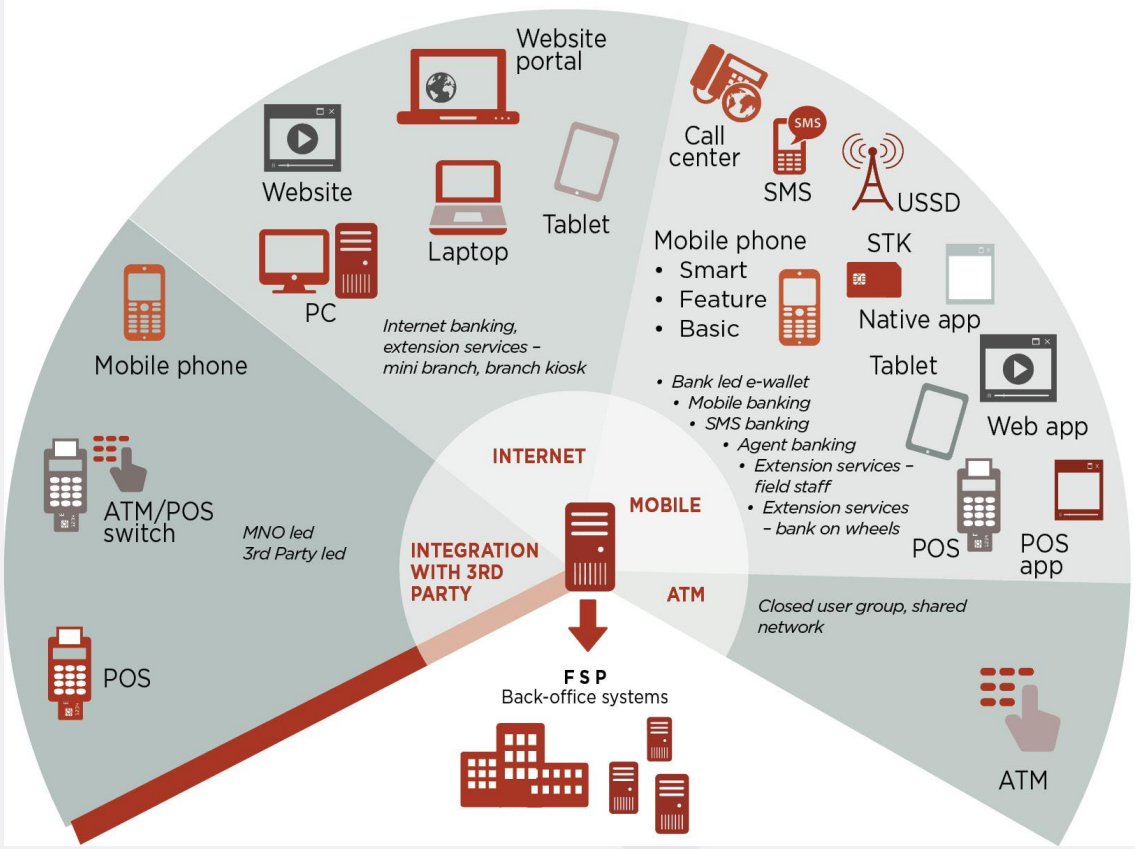
ADC Back Office: Integration

Back office should cater for all user administration/customer registration, authentication process, reporting, reconciliation, monitoring performance etc.

Integration between systems involved in the ADC platform.

- Existing systems (MIS, CBS, Accounting/Finance, ERP)

- 3rd Parties (m-wallet providers, bulkd SMS providers, payment aggregators, national switch)



ADC Back Office: Communications

Communications - All ADCs ultimately require the exchange of financial or non-financial information between the FSP and the customer, which typically occurs over communication channels connecting the device and the back-office component of the ADC

Communication Options	
Local area network / wide area network (LAN/LAN)	Internal network used to communicate between devices branches, etc. Could be leased line, wireless, satellite, VPN
Internet portals	Secure web application used to exchange information. Typically requires credentials to access
Mobile data	MNOs offer mobile data services (GPRS, Edge, 3G or 4G4), to access to the web and exchange information.
USSD	Unstructured Supplementary Service Data use interactive session consisting of a two-way exchange of messages
SMS	‘Store and forward’ communication channel that uses SMPP protocol to send a limited amount of text from one phone to another, or from one to many phones
Interactive Voice Response (IVR)	Computer application with voice recognition technologies and keypad tones during an interactive phone call
Near Field Communication (NFC)	Standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart

SoftwareGroup
doing it right

ADC Back Office : Authentication

FACTOR TYPE	DEFINITION	OPTION AVAILABLE
Knowledge	*Something that customer knows*	*Password, PIN, pattern, secret question, image*
Possession	*Something that customer owns or has*	*Bank card, mobile phone, OTP/TAN, physical ID card*
Inheritance	*Something that customer is*	*Biometric characteristic fingerprint, iris scan*

Transactions initiated remotely through ADCs often require enhanced means of verification.

Best practice for authentication over ADCs dictates that two-factor authentication should be used.

The level of security delivered will be influenced not only by the number of factors used in authentication but also by the relative security of the factor itself.

SoftwareGroup
doing it right

ADC Risks

Five risk areas to consider with ADC projects

1. **Legal**- risk of lawsuits arising due to misuse of the channel, breach of contracts or laws such as data protection and AML, immature governance structures
2. **Operational**- fraud /theft committed via the channel, agent/ATM liquidity management, poor quality of service, unauthorized fees
3. **Technological**- logical and physical security, lack of integration, software/hardware failures, weak support + implementation from suppliers
4. **Compliance**- risk of fines or loss of license due to non compliance with laws including AMK, CFT, Agency, e-money, consumer protection, regulatory reporting
5. **Reputational**- loss of customer and market share due to the occurrence of any of the above risk. Can be higher where using third parties to represent the bank and don’t adequately control the quality of service from these agents.

SoftwareGroup
doing it right

ADC Technology Implementation Process

SoftwareGroup
doing it right

Phase 1: Define Channel Strategy

Step 1- Define the ADC objectives

Vision/mission/strategy of FSP, strategic objectives, identify channel strategy team

Step 2- Assess the environment

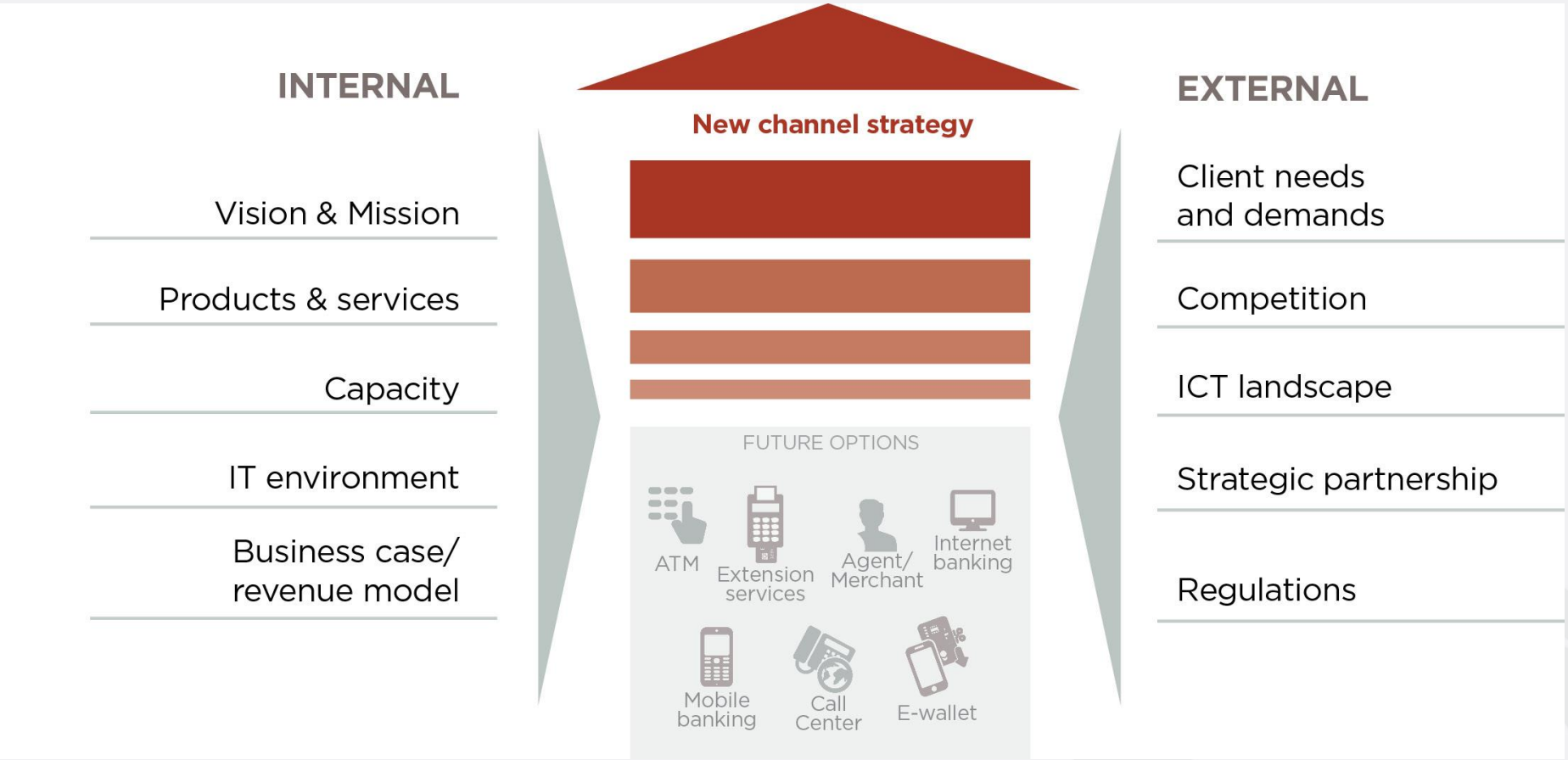
External and Internal Assessment

Step 3- Develop the channel strategy and business case

Business goals/objectives for the channel, market analysis, SWOT analysis of channels, recommended channel, requirements (ops, financial, IT), high level timeline, high level budget, risk analysis

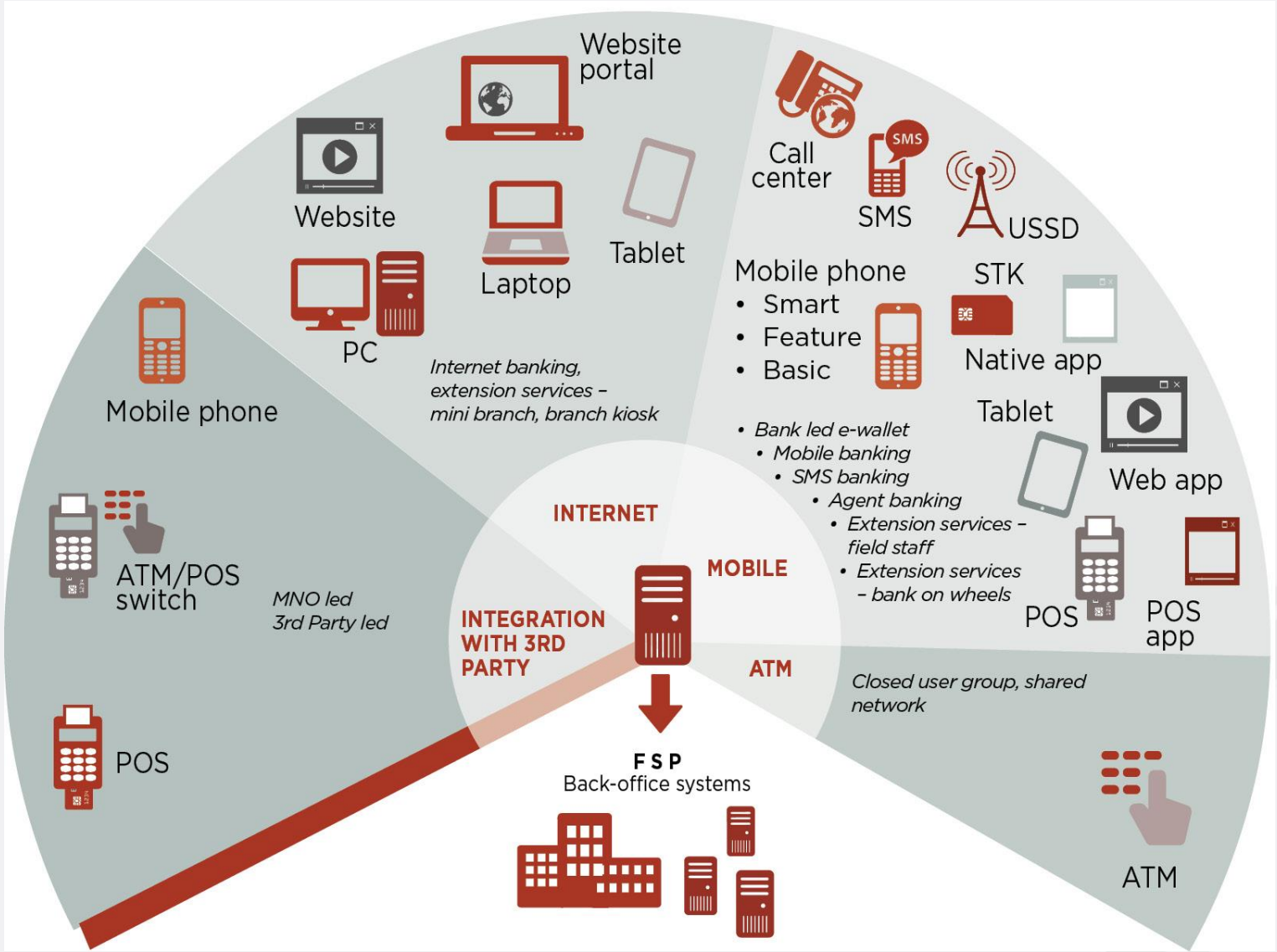
SoftwareGroup
doing it right

Phase 1: Define Channel Strategy



SoftwareGroup
doing it right

Phase 2: Map Strategy to Tech Platform



SoftwareGroup
doing it right

Phase 2: Map Strategy to Tech Platform

Step 5- Gather influencing criteria

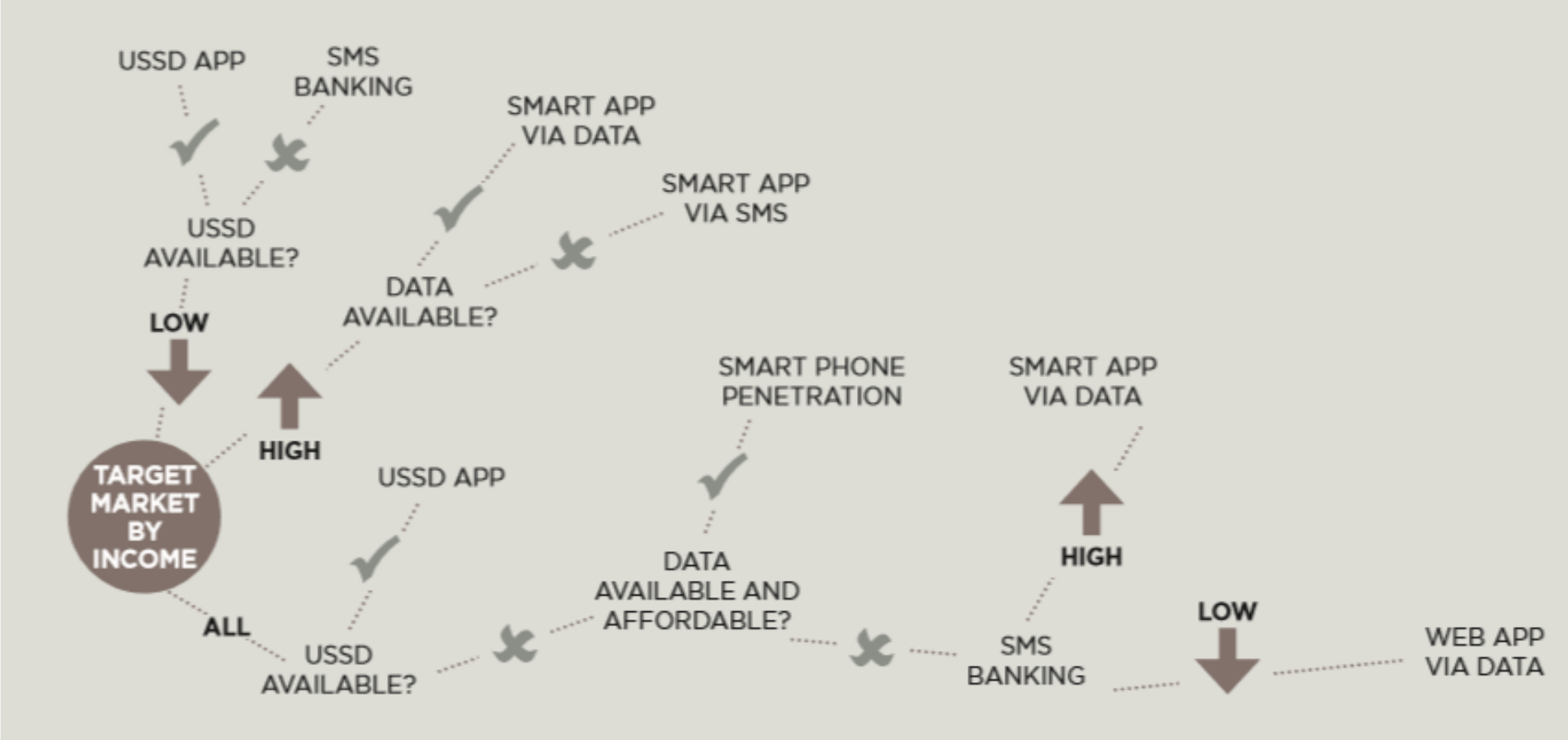
- Types of transactions
- Security levels
- Mode of authentication: card + PIN, biometric, OTP
- Quality/availability of communication channels
- Handset availability

Step 6- Select the platform

Consider the advantages and disadvantages of the various applications and device options

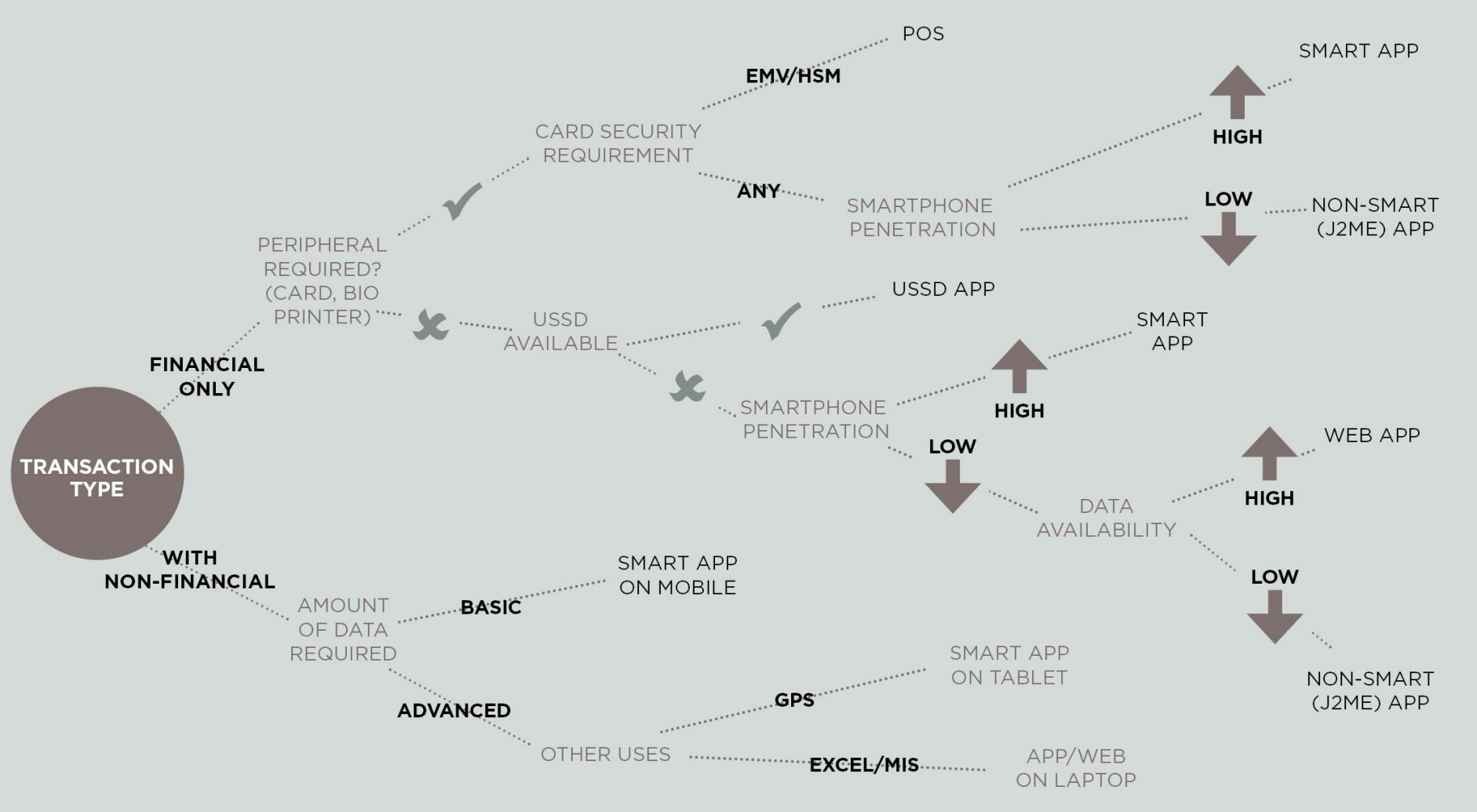
SoftwareGroup
doing it right

Phase 2: Map Strategy to Tech Platform Decision Tree: Mobile Banking



SoftwareGroup
doing it right

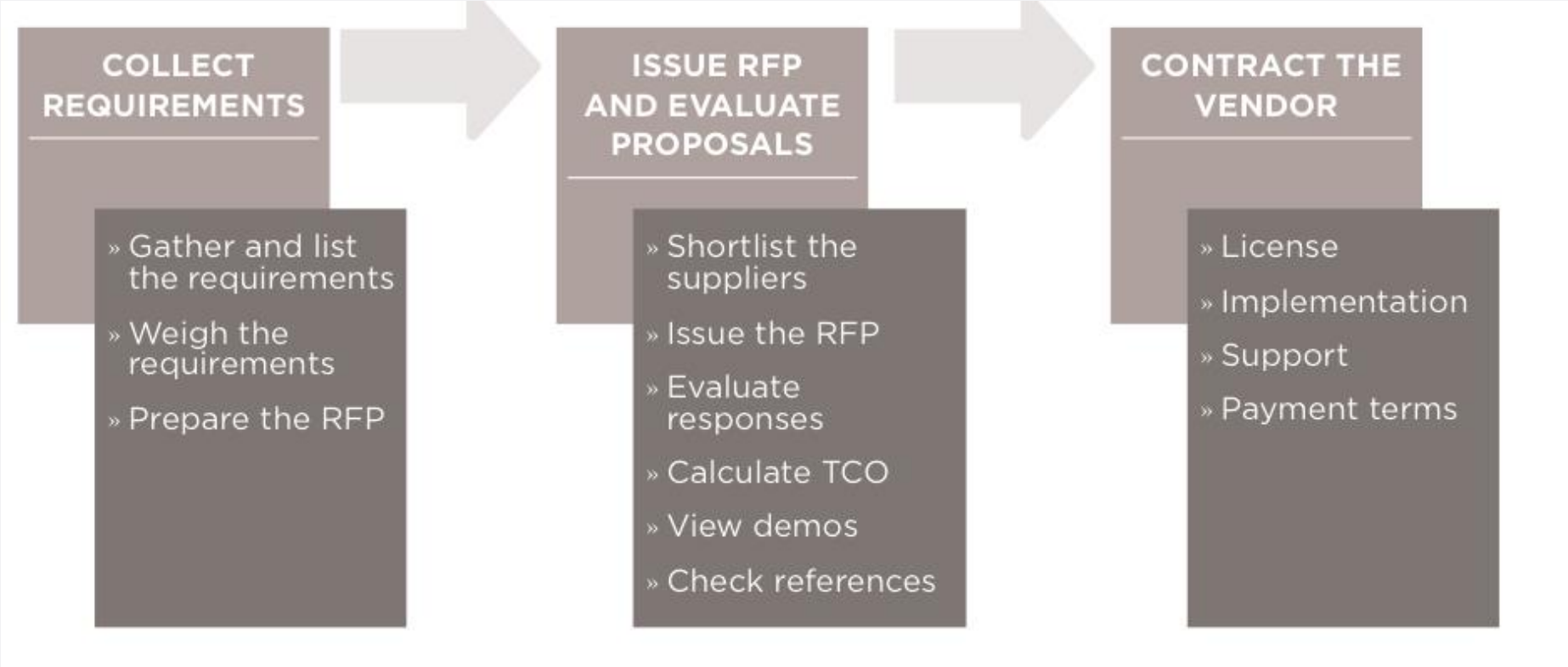
Phase 2: Map Strategy to Tech Platform Decision Tree: Agency Banking



SoftwareGroup
doing it right

Phase 3: Vendor Selection

Step 7- Collect the requirements
Step 8- Issue the RFP and evaluate
Step 9- Contract the Vendor



Stage 4: Implementation

Implementation Process

SoftwareGroup
doing it right

Step 4: Implementation- Decisions

TECHNOLOGY	KEY IMPLEMENTATION DECISIONS
	• *Which bulk SMS provider to use for both sending SMS and short code (required for pull mesages).* • *Confirm maximum message length for SMS from the bulk SMS provider.* • *If short code needs to be accessible across multiple networks, need to identify which authority can allocate a single number.* • *Where to store customer's phone number: in CBS / mobile banking system or other system.* • *How to register / subscribe customers for the service? Automatically versus on request.* • *Where to configure fees if charging for the service: in CBS of mobile banking solution.* • *SMS message definition – decide what text to send, when to send it and in which languages.* • *How to add / change messages over time.*
ATM	• *Join existing third party ATM network or launch own.* • *Closed user group or integrate to other payment networks: national switch, Visa, MasterCard.* • *Which system to apply the authorization policy and the rules of this policy.* • *Which system to store business logic such as limits and fees.* • *If own network: decide re hardware procurement, device management systems, liquidity management.* • *Configuration of card management – card production, administration, support, authentication management, HSM, card printers.* • *Reconciliation and settlement – policy and systems used to support.* • *Definition of screens and states (and in what languages).* • *Setup of an ATM help desk.* • *If joining other network: how to integrate> What connectivity required and how to test and settle / reconcile.*

SoftwareGroup
doing it right

Step 4: Implementation- Decisions

INTERNET BANKING

- *How to do customer authentication: one factor, two factor, security tokens, TANs, pictures, passwords.*
- *How to register customers for the service.*
- *What systems to support on-going administration of channel i.e. help desk.*
- *Workflow automation for processes originated via internet – check book requests, loan applications, high value transactions, currency exchange.*

AGENCY

- *Whether to print transaction receipts or use SMS .*
- *How to manage the devices used by remote users: MDM versus other device management system.*
- *How to manage agents including limits, commissions, access rights, liquidity and float accounts.*
- *Whether to support both online and offline processing: offline for non-cash, all cash online.*
- *If offline, what criteria to use to sync data: loan officer, region, other.*
- *KYC implications on remote account opening.*

M-WALLET INTEGRATION

- *How to match incoming payments to the correct customer account i.e. which identifier: phone number, national ID, account number.*
- *What business rules to apply to incoming payments: overpayments, group accounts, split to savings.*
- *Outward payments – how to validate a customer's phone number: one-off registration versus confirmation at time of sending.*
- *How / when to reconcile payments between the systems: automated versus manual, daily.*
- *Receipting payments received via M-wallet: manually versus SMS versus no receipt.*
- *How to handle group loans over this channel: individual versus batch.*

Step 4: Implementation- Decisions

M-BANKING

- *How to register customers for the service.*
- *Where to store customer's phone number: CBS or m-banking system.*
- *How to support PIN setup and administration.*
- *Where to configure fees if charging for the service.*
- *Process flow per transaction type.*

BIOMETRIC CARD

- *Enrollment process – new and historic customers.*
- *Maker / checker versus one person enrollment.*
- *Accessibility of bio verification across all systems – CBS + channels.*
- *Exception process – what happens if it does not work.*
- *Deduplication process – when to run these checks, process to follow up if duplicate found.*
- *Which fingers to capture.*
- *Which model of reader to use.*
- *Number of allowed attempts to authenticate.*
- *FAR / FFR thresholds**
- *Catering for change to business process: who to capture, cashier processes.*
- *Different types of cards – smart, mag, EMV.*
- *Card administration as the application, processing and on-going management of the card for the customer.*
- *Card production is the physical creation of the card, which is often done by an entity other than the one doing administration.*
- *First decision is who will administer and produce the cards.*
- *Pre-printed versus customized-pros / cons.*
- *PIN management – HSM, PIN mailers.*
- *Card helpdesk support.*

** Using biometrics in any business requires an appreciation of the performance metrics by which the systems are measured, particularly the False Acceptance Rate and False Rejection Rate. FAR, also known as False Matching Rate, is the rate at which the system incorrectly accepts the wrong person at the point of verification. By contrast, FRR is the rate at which the right person is wrongly rejected by the system due to a failure to match their authentication details with the stored record. FAR and FRR rates have an inverse relationship with one another. In other words, the more selective the biometric system is (a better FAR rate), the more likely it is that the system will also begin to occasionally reject the correct fingerprint. Biometrics systems will need to be configurable to decide the best setting to use to balance these two rates, which is both a function of the size of the database as well as some individual system factors that a vendor will need to advise on.*

PIN

- *Registration.*
- *Who / where to reset PINS.*

SoftwareGroup
doing it right

Lessons Learnt

1. Use existing networks to test out new channels
2. Challenge your existing processes to maximize impact
3. Pick partners carefully
4. Prioritise flexibility and scalability
5. Consider the context carefully
6. Accept that strategy will evolve over time

SoftwareGroup
doing it right

About Software Group

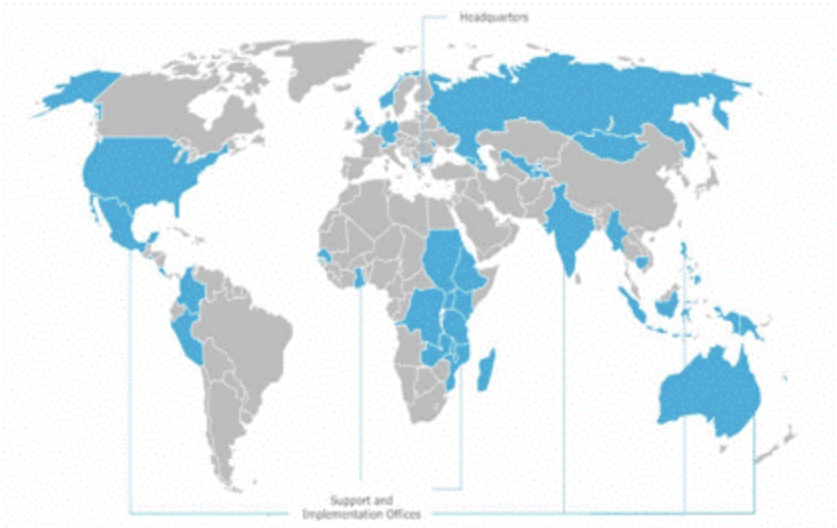
Software Group is an advanced technology company focused on end-to-end solutions for the financial and retail sector.

The experienced team of professionals is committed to the efficient delivery of innovative solutions and has an outstanding track record of handling complex development projects.

Software Group prides itself on delivering products and services which adhere to the principles of quality, transparency and affordability.

SoftwareGroup
doing it right

About Software Group



With 7 offices and 14 partner support offices we serve over 100 clients on 6 continents

Products, Services and Solutions

IT Strategy
Consultancy, assessments, selections, implementations, audit, enhancements, support

Delivery Channels and Agent Networks
Design, development, implementation, utilities building

Reporting and Analysis Tools
Products, design, development, implementation, support

Integrations
Design, development, implementation, support

Mobile Banking and M-Wallet
Products, design, bespoke apps development, implementation, integrations

SoftwareGroup
doing it right

Product Portfolio

- EFT Switch
- EFT Bridge
- Web front-end for banking system
- Mobile banking / M-wallet application
- SMS messaging and alert platform
- Card Management System
- Biometric authentication
- Data Warehouse

SoftwareGroup
doing it right

Main Solutions

Agency Banking

Deploy an agent network to support low cost expansion of services

Digital Field Application

Access your MIS/ERP/CRM from the field through use of mobile applications to digitize your operations

Mobile Banking

Enable mobile access for customers to transact and enquire anytime, anywhere.

Web Front End

Deploy a web based front end for financial institutions that supports the full customer lifecycle

Payment Gateway

Integrate with any type of 3rd party network, settlement and reconciliation

Biometrics

Capture, search and verify identity using biometrics

Alerts and Campaigns

Efficient customer communication via SMS or E-mail

Data Warehousing

Same data different view, extract and deliver reports that meet your business needs

ATM&POS Management

Develop and operate your own ATM/POS network

Card Management

Issue and operate debit and credit cards, prepaid cards, etc.

Internet Banking

Provide clients with a convenient channel to manage their accounts

M-wallet

M-wallet system for banks, mobile operators or third party providers

Bank Reconciliation

Supports reconciliation and settlement between multiple parties

Anti-Money Laundering

Web based solution for monitoring, control and compliance

Remittance Management

Full support of non-account money transfers

SoftwareGroup
doing it right

Thank you!

Contact Us

SG Headquarters, Europe:
115N, Tzarigradsko shosse blvd.
1784, Sofia, Bulgaria
+359 2 923 17 83

Sub-Saharan Africa:
Suite 14, The Green House
Ngong Road 28804-00100
Nairobi, Kenya
+ 254 717 639 392

West Africa:
Fayza Plaza 2nd Floor, Apartment No.3
Oyarifa Accra, Ghana
+233 302 975617

Asia:
5/F La Paz Center, V.A. Rufino St,
Makati, 1128 Metro Manila, Philippines
+63 2 831 1424

Pacific:
4/36 Agnes Street
Fortitude Valley, 4006, Australia
+61 732173249

Latin America:
Av. Venustiano Carranza 1041
Zapopan, Jalisco, 45180, Mexico
+52 1 331 3317513

www.softwaregroup-bg.com
info@softwaregroup-bg.com