IT Risk: Mobile Banking and Payments

Agenda – Purpose of Presentation

- Define Mobile Financial Products
- Describe Mobile Banking functionality, drivers and risks
- Describe Mobile Payments functionality, drivers and risks
- Identify the key supervisory practices for understanding and evaluating mobile financial products

Mobile Financial Products

Current and Emerging Payment Models

Business models under development

1. Network operator centric (e.g. Verizon)
2. Bank centric
3. Managed by a trusted third party (Google, Paypal, Square, etc.)

"Major players" category is getting crowded

- Mobile network operators
- Handset / SIM chip manufacturers
- Banks
- Card associations
- Payment networks
- Prepaid companies
- Merchants
- Internet search and payment services providers
- Proprietary payment application providers

Business Drivers

Value add

- Potential for scale in fragmented markets
- Ability to focus on new markets (unbanked, under-banked)
- Innovation that bypasses current infrastructure limitations
- Major influence on efficiency and access to payment services

Business Challenges and Risks

Challenges/Risks

- Unclear regulatory oversight in emerging markets
- Potential unintended consequences – risk, fraud, security
- Data governance and vendor management
- Unclear impact on consumers when innovations or innovators fail
- Unclear responsibility for regulatory oversight / consumer protection
- May create a major single point of failure potential

Mobile Banking

Mobile Banking (insured depository institutions)

Use of a mobile device

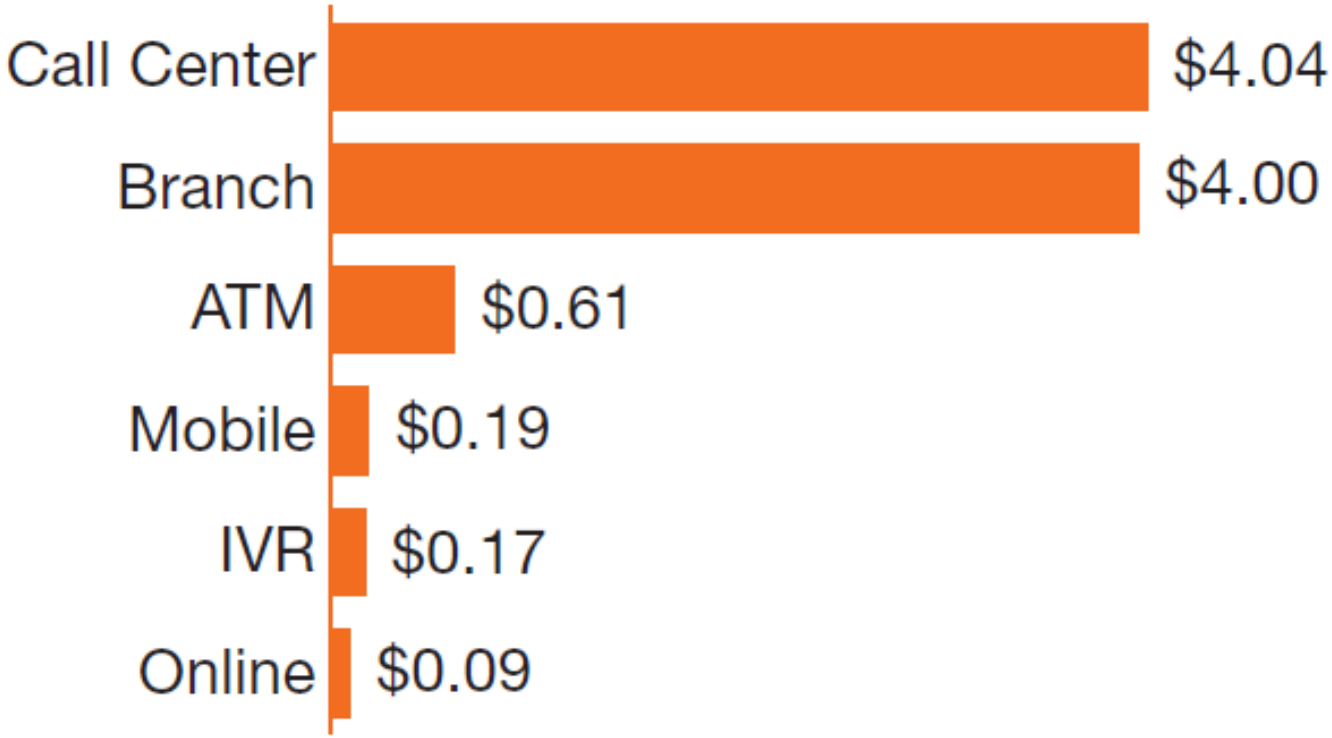
- cell/smart phone or
- tablet computer

Conduct banking activities such as

- balance inquiry
- account alerts
- bill payment

Transaction Costs by Banking Channel

Average transaction cost in the US
(includes labor and IT costs)



Source: CEB TowerGroup

Mobile Application Types

Native Client

Application and Application data reside on device.

Using the language and platform of the mobile device.

Hybrid Client

Application Resident on device; data sourced from “online” sources.

Browser embedded within the app, based on HTML5.

e.g., Netflix, Linkedin, Facebook, Yelp, etc.

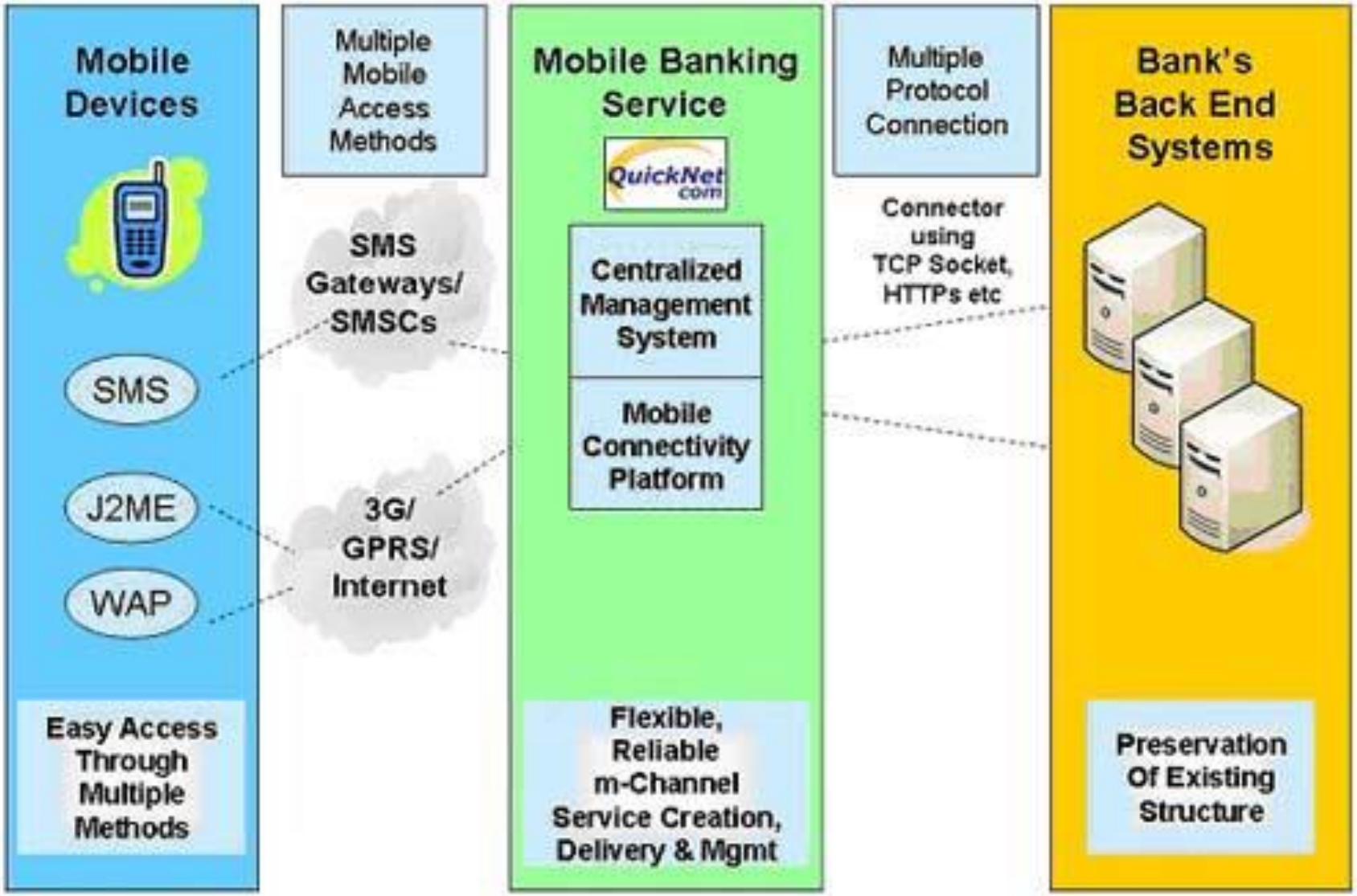
Web Client

Neither application nor data reside on device.

Browser or small downloadable client.

Supports also older phones.

Integration with Existing Infrastructure



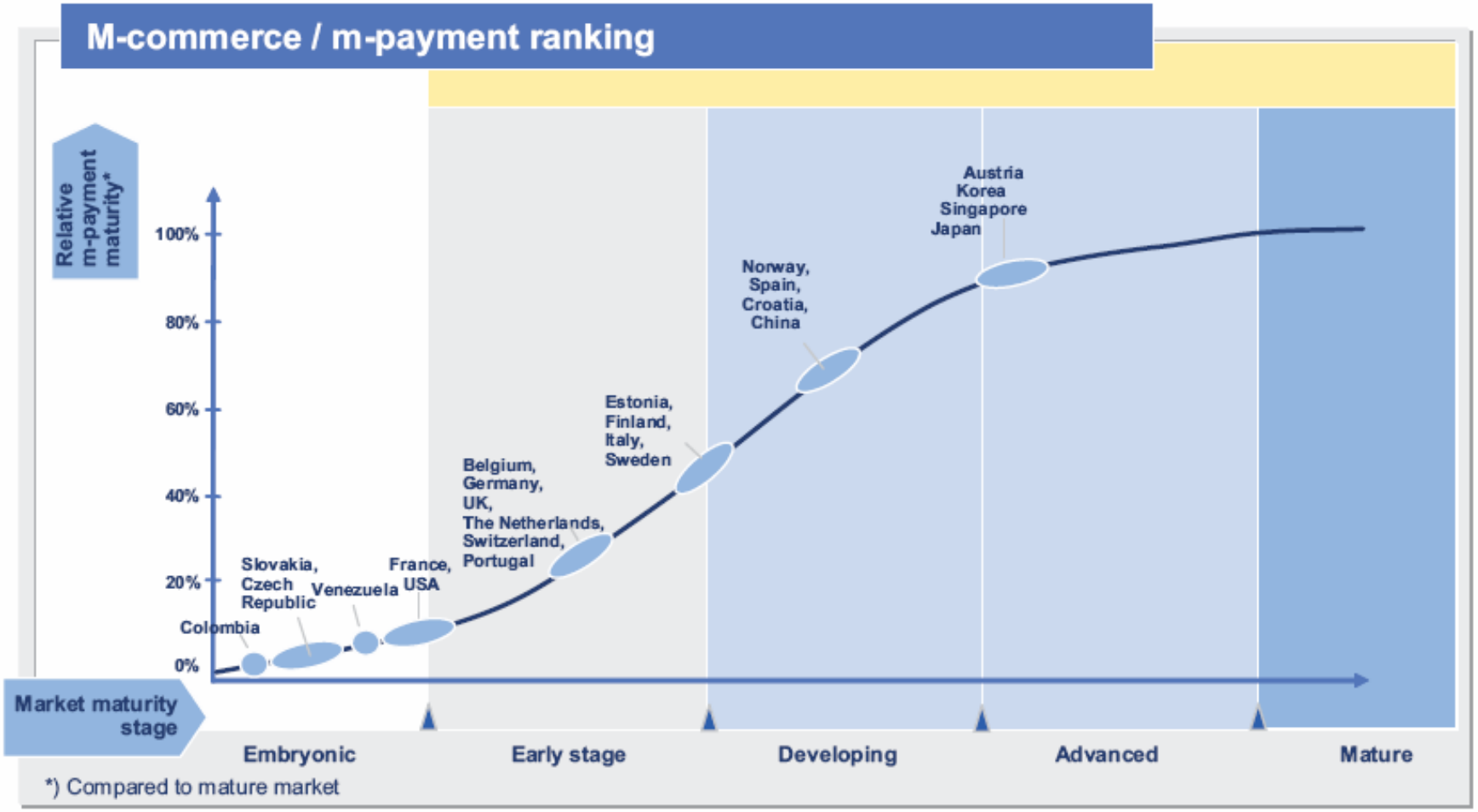
Mobile Payments

Mobile Payments (many types of companies)

Mobile banking and payments are not interchangeable

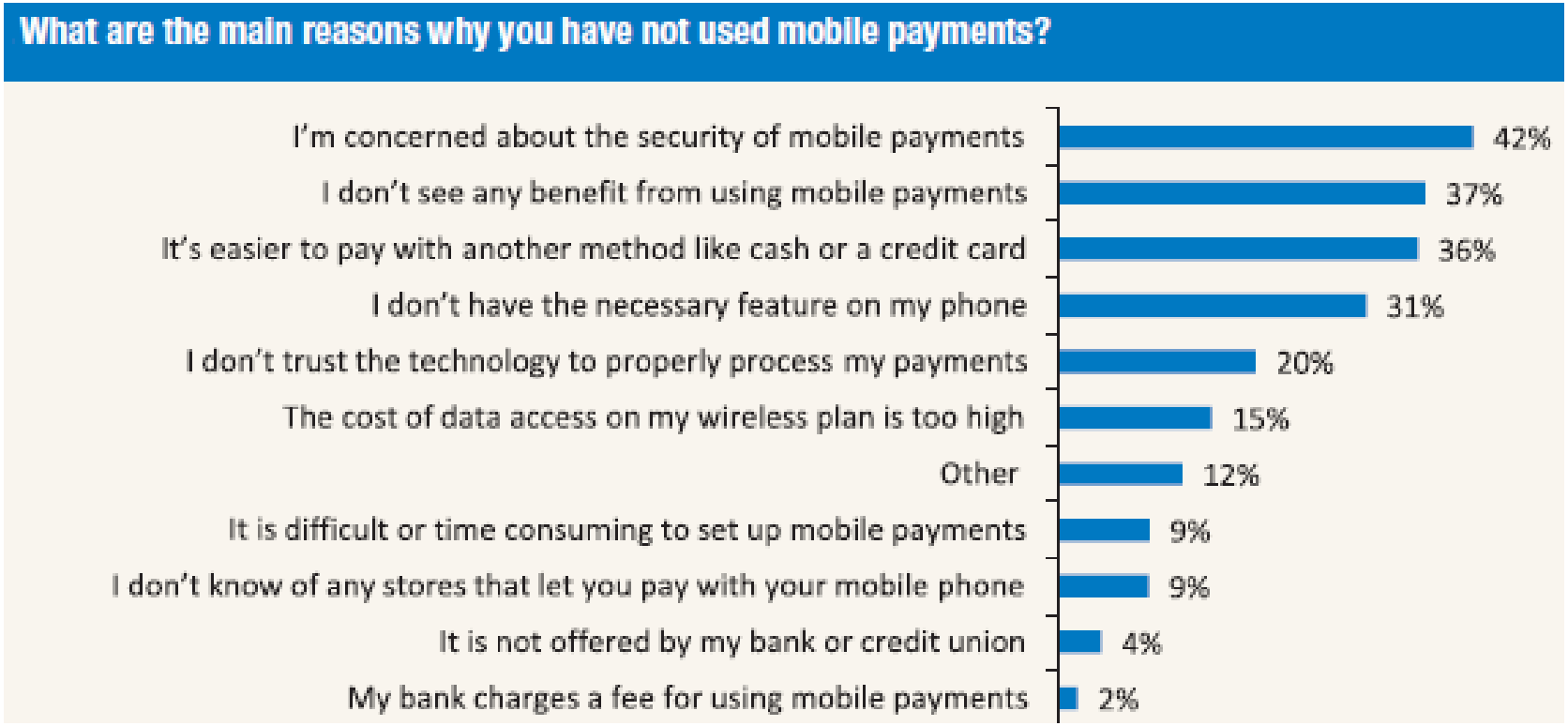
- uses the same mobile devices to initiate payments
- from a person to person(s) or businesses

Global Mobile Commerce Rankings



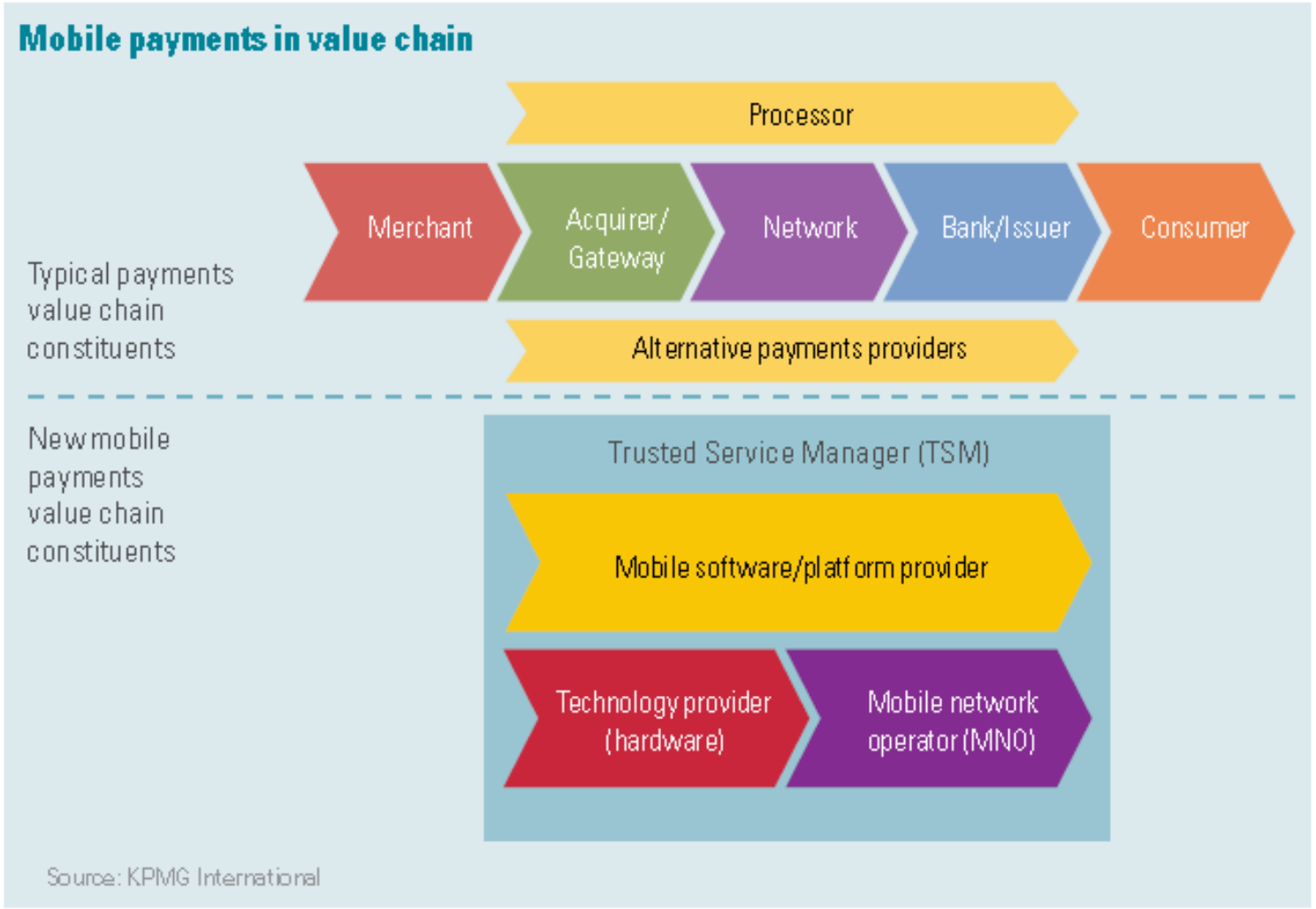
Source: Arthur D. Little M-Payment Report

Customer's Perception



Source: Consumers and Mobile Financial Services Study (Board of Governors of the Federal Reserve System – March 2012)

Mobile Payments in Value Chain

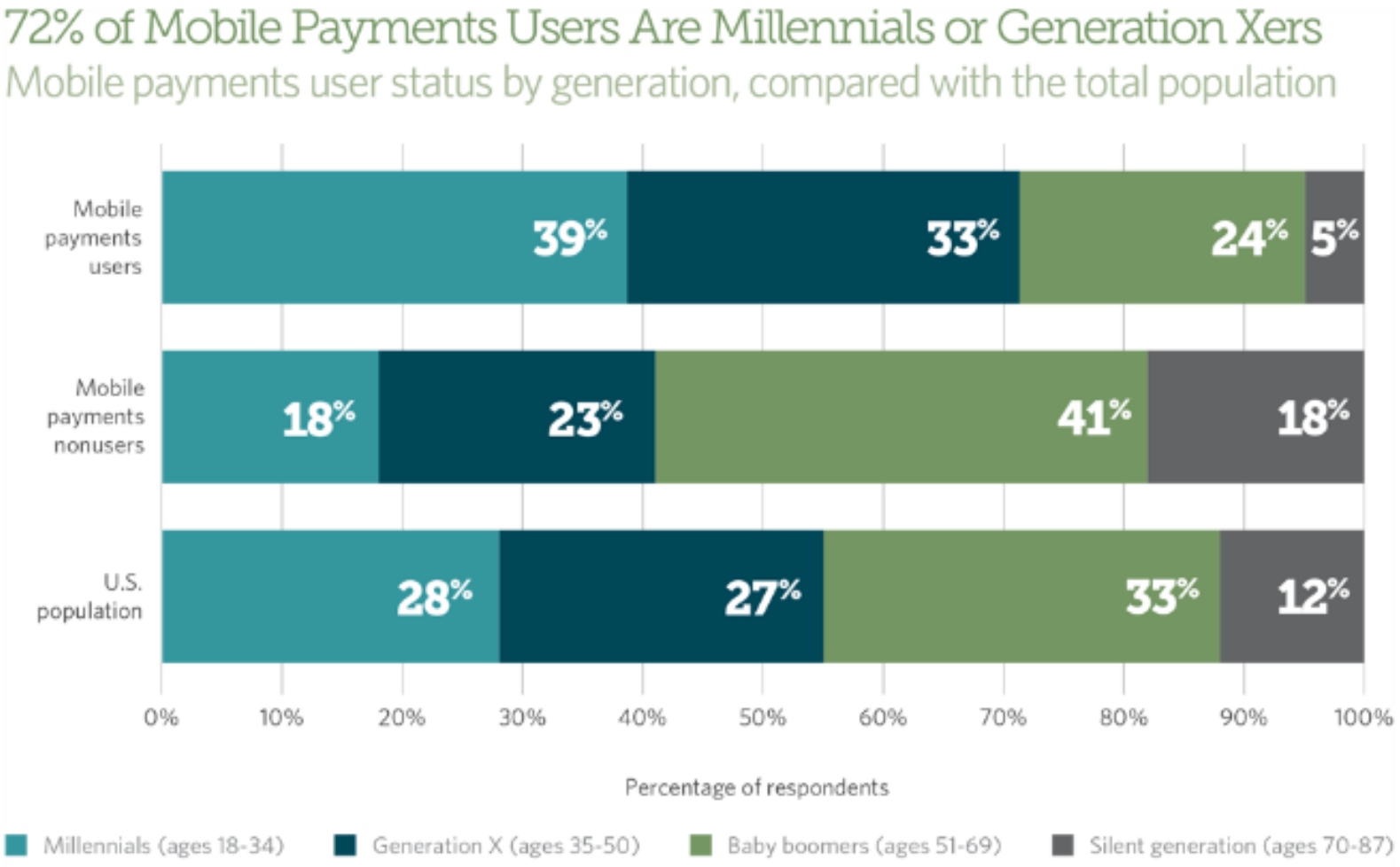


Mobile Payments

Mobile payment technologies			
NFC companion devices	Enables contactless proximity payments at merchant POS terminals using a range of technologies such as stickers, fobs and microSD cards.	Leverages existing contactless card standards, enables payments without MNO cooperation.	Devices often limited to a single payment account, potentially high initiation complexity for user, requires distribution and device costs to be absorbed.
Embedded NFC	Uses a mobile wallet technology on an embedded NFC chip to broaden payment options within a proximity setting.	Uses existing contactless card standards, enables access to multiple accounts via mobile wallet interfaces, provides some additional security with PIN on the handset.	Limited availability of enabled handsets in the market, MNOs control handset inventory and distribution.
SMS text	Remote payments, primarily for digital content.	Ubiquitous capability available on the vast majority of handsets.	Message length limited, high cost to both merchant and consumer, many jurisdictions do not allow SMS for mobile payments.
Voice	A niche technology that provides mostly account servicing and bill payments, some mobile payment authorisation conducted via voice.	Person to person interaction, opportunities for dynamic cross-selling.	High cost in 'live agent' situations, inefficient data communications.

Source: KPMG International 2011

The Mobile Payments Generation Gap



Establishing Mobile Security Policies

- Define the policies from a threat and controls perspective:
  - Utilize existing policies and standards for guidance
  - Align to corporate policies, industry standards, and applicable regulations
- Consider the policy impact on business functions and user experience
- Align policies with capabilities of management solutions
  - Identify what policies can be enforced, and how policies are managed and pushed
  - Consider how enforced policies will be tested and validated
  - Consider the impact of policies on security administration and supporting infrastructure
- Adopt multiple policies for differentiated use cases as needed; limit where possible.

Key Mobile Policy Elements

- Data Storage
- Data Sharing
- Device Connectivity
- Device Authentication
- Data and Device Wipe Mechanisms
- Feature Controls
- Applications Allowed

Supervisory Considerations

- Controls over mobile product development including interoperability of complex mobile payment systems
- Controls over 3rd parties including non-bank partners, networks, vendors, and service providers including RFP approach and SLAs
- Coverage over legal and compliance risks
- Implementation of customer exposure limits including fraud detection and response plan
- Implementation of Security and customer education requirements
- Transaction authentication and authorization practices