EMERGING PAYMENT AND MONEY MANAGEMENT OPTIONS: DEFINITELY CONVENIENT BUT ARE THEY DANGEROUS?

2012 Consumer Issues Conference
University of Wyoming
Oct. 4, 2012

General Topics
1. Overview of Mobile Payment and Money Management Options
2. Emerging Mobile Payment Alternatives
3. Limitations & Consumer Concerns
4. Rules & Regulations

Overview of m-Commerce
- Mobile commerce (m-commerce or m-business) is any eCommerce activity done in a wireless environment through a handheld mobile device.
- Can be done using mobile phones, smart phones, notebooks, iPads, smartpads, and anything connecting to the Internet.
- Creates opportunity to deliver new services to existing customers and to attract new ones.
- Encompasses many areas involving e-Commerce including mobile payment, money management, and other areas. The technology has been in use for 10 years, but it is really only taking off now with smart phones and tablets.
- North America has been much slower to adopt than many areas in Asia (Japan & South Korea for example)

Octopus
Hong Kong
Since Sep 1997
- To pay, wave an Octopus card within a few centimeters of the reader (even if it’s in a wallet/purse)
- Audio-acknowledgement (beep)
- Display of total amount and remaining balance
- On MTR and KCR transport, the total amount is calculated from the entry and exit points

Japanese Mobile Wallet (Osaifu-Keitai)
- Many Japanese mobile phones contain an extra chip, which uses RFID/NFC to communicate with payment-related devices
- Services include:
  - eMoney (Edy)
  - public transport (Mobile Suica)
  - vending machines
  - Loyalty cards
RFID Tags for Road-Tolls

- Car requires a transponder
- Car drives through a control point
- The fee can be shown on a static or variable display
- The control point interacts with the transponder, and the toll is deducted automatically
- There is audio-acknowledgement of transaction
- Depends on blind consumer trust

EARLY CONTENT AND APPLICATIONS HAVE BEEN GEARED AROUND DELIVERING INFORMATION, BUT REVENUE GENERATION IS INCREASINGLY BECOMING THE FOCUS!

Entertainment
- Music
- Games
- Graphics
- Video

Money Transactions
- Banking
- Stock trading
- Shopping
- Auctions
- Reservations
- Betting
- Mobile wallet
- Mobile pay

Communications
- Short Messaging
- Multimedia Messaging
- Unified Messaging
- e-mail
- Chatrooms
- Video - conferencing

Information
- News
- City guides
- Directory Services
- Maps
- Traffic and weather
- Corporate information
- Healthcare

Online commerce

EARLY CONTENT AND APPLICATIONS HAVE BEEN GEARED AROUND DELIVERING INFORMATION, BUT REVENUE GENERATION IS INCREASINGLY BECOMING THE FOCUS!

Generations
- 1G: 1979-1992 wireless technology
- 2G: Wireless technology accommodated text and graphics
- 3G: 3rd generation technology (2001-2005) supports rich media (video clips)
- 4G: provides faster multimedia display (2006+)

The Realities of Mobile Payment

- Direct payment systems have developed like NFC (near field communications), mobile wallets, and mobile apps.
- Services are striving to make online shopping even easier by lumping payment methods, loyalty cards, and coupons all into one location. (Examples: Google Wallet, Passbook, and ISIS)
- Retailers such as Walmart, Target, and BestBuy jumping into the game with Merchant Customer Exchange (MCX).
**Facts and Figures**

*M-commerce*

- Only 10% of consumers bought goods and services via a mobile device in 2008. By 2010, this figure increased to 28%.
- Juniper estimates that mobile payments will account for more than $1.3 trillion in transactions by 2017 on a global level.
- It is expected that the U.S. alone will total $170 billion.
- Juniper Research estimates that the number of people paying for goods and services through their mobile devices is expected to reach 2.5 billion globally.
- Overwhelming number of consumers worried about the security of their personally identifiable information.

**Attributes of M-Commerce and its Economic Advantages**

- Mobility
- Broad reach — reach someone any time
- Ease — real-time access to information
- Convenience — devices store data and enable instant Internet connection
- Personalization — prepare information for individual consumers
- Localization of products and services — know where the user is located at any given time and match services to them.

**Mobile commerce from the consumer's point of view**

- Consumers increasingly use cell phones, smart phones, tablets, and other mobile technology to engage in commerce.
- Consumers want to access information, goods and services any time and in any place on their mobile devices.
- Use a mobile device to purchase tickets for events, ride public transportation, order at a restaurant, park, download content, search real estate, and do almost anything.
- Websites should be tailored for optimized mobile browsing.
- The consumer should be offered suitable payment methods.

**Mobile commerce from the provider's point of view**

- Enhances business opportunities
- Must be confident about technology and sure that the payment is made, traceable, and secure.
- Must adequately inform customer what is being bought, how much to pay, and payment options.

**M-Commerce Basics**

- **P2P payments**
  - Traditionally: Person-to-Person payments, limited to cash and checks.
  - Use an iPhone or iPad to send funds from debit or credit accounts (Mastercard).

- **C2B payments**
  - Traditionally: Consumer to Business payments. Done through cash, credit, debit cards, electronic bill paying, and wire transfers.
  - New: Consumers pay businesses using technology.

**Multiple participants**

- Hardware, software, transmission, payment, sales, etc.

**Overview of the participants**

- **Hardware:** controls the technology and capabilities of the end-device
- **Software:** develops the means of implementing a mobile payment infrastructure by producing a software that connects all parts of the payment process.
- **Mobile network operators (MNO):** operate the wireless networks through which communications flow. [Verizon, AT&T, Sprint]
- **E-commerce participants:** typically need to collaborate with financial institutions including banks, credit card companies, PayPal, and even utility companies to obtain payment.
Text messages illustration

Send a text to a financial institution instructing them to perform banking functions or receiving a message about a deadline.

- Very convenient, but there are disadvantages
  - Limited number of characters
  - Risk of mistake ($20.00 versus $2000)
  - Lack of encryption and user authentication
  - Fraud through techniques such as phishing
  - Infection by viruses

Mobile phone surfing

- Wireless applications on cell phone browsers, smart pads, or software downloads
  - All of the advantages of online banking or shopping from a home computer

- Disadvantages include:
  - Minefield of malicious links
  - Fraud
  - Mistake

Tablets

- Tablets mainly differ in the size of the screen, but they share the same software, operating systems, and processors so their security concerns are nearly identical.
- About the only difference is that some tablets can use USB devices, which increases the attack surface of such devices.

Payment Options

What is the major impact to consumer and corporate payments will be?

- Traffic annually up over 200%
- Licensed as a “money transmitter” in over 40 states; not regulated as a bank so minimal regulatory protections.
- Aggressively partnered with companies that offer electronic commerce platforms to merchants so that consumers can offer their PayPal accounts.
- PayPal allows application and software developers to access its platform.
- iPhone app allowing customers to order pizza and pay using their PayPal account
Square claims 2 million customers
Anyone can process credit cards
Spawned copycats including Intuit (GoPayment), mPowa (PayAnywhere), and PayPal's triangle device. Differences include rate charged and flow of money.
Pay with Square now allows consumers to pay by activating an app on their iPhone which transmits the consumers face to the cash register when you are in the store.

Limitations of M-Commerce

- **Usability Issues**
  - Mobile devices are small (screens, keyboards, etc) making it difficult to see full web addresses and e-mail addresses. This increases the chances of fraud.
  - Difficult to browse websites
  - Limited storage capacity
  - Click on the wrong button

- **Technical Issues**
  - Lack of a standardized security protocol
  - Insufficient bandwidth
  - Cost
  - Poor reception / Weather and terrain issues
  - Battery limitations and power outages

Security, Privacy & Other

Security issues

- More than 2 million smartphones reported lost each year.
- According to a recent Juniper Report, more than 76 percent of consumers surveyed use their smartphones or tablets to access sensitive personal or business information. Among these ...
  - Over 50 percent of these consumers entered or modified passwords;
  - 43 percent accessed banking or credit card statements;
  - 30 percent to access utility bills;
  - 20 percent shared financial info (credit card numbers, etc.);
  - 18 percent accessed employer’s proprietary information;
  - 17 percent accessed medical records; and
  - 16 percent shared social security numbers.

Security issues

- With unit sales of smartphones and tablets eclipsing those of desktop and notebook PCs, cybercriminals increasingly set their sights on mobile devices and mobile Internet use.
- A security breach for businesses can be devastating: cost of audit, fines from government agencies, reputation, and lawsuits even.
- Payment systems example: in April 2012, one of the biggest names in digital and mobile commerce, Global Payments, confirmed a significant security breach affecting 1.5 million credit card holders. Within days, Visa dropped the company from its list of security compliant providers.
Security issues & Healthcare
- Health care professionals and their patients must guard against the dangers inherent in m-commerce.
- There is so much new technology that we are just learning the risks. Some of the potential problems include:
  - Doctors who lose iPhones and other mobile devices containing patients’ personal data
  - Hackers potentially killing patients who rely on implanted devices, such as pacemakers or glucose infusion devices.

Security: the technical side ...
1. Most Internet-enabled cell phones in operation are incapable of storing applications meaning that they cannot propagate a virus, worm, or other rogue program from one phone to another.
2. Most cell phones have their operating systems and other functionalities “burned” into the hardware making it difficult for a rogue program to permanently alter the operation of a cell phone.
3. However, as the capabilities of cellular phones have increased and the functionality of smart phones and cell phones have converged, the threat of attack from malicious code has increased.

Security: Increase in Malware
- Nearly 7 out of 8 attacks on smartphones come on the Android platform

Security: Second party threats
- June 2010 ... AT&T customers accessing their accounts to order an iPhone saw details of other customers.
- Data stolen by merchant

Security: Third party security
- Most third party applications and mobile add-ons have not been thoroughly checked for security holes, which hackers can and do exploit to steal personal data
- Several apps on Google’s Android system removed based on suspected fraud and theft of financial information
  - SMShing virus infects mobile phones giving them potential access
  - Fraudsters placed program on Nokia phones that generated small monthly charges on wireless account
- Phishing in an anonymous world
- Lost or stolen phones
- “Jailbroken” phones

Privacy Measures
- Privacy policy
- Selling or otherwise using data (third party advertisers)
Privacy Policies and Disclosed Practices:
Information Shared With Third-Parties

Companies insert statements in privacy policies about who they would share consumers personal information with such as the following:

- "to perform business support functions on our behalf"
- "for the purposes of . . . improving the user experience"
- "to companies that provide services to help us with our business activities such as shipping your order or offering customer service."
- "to strategic partners . . . that help . . . market to customers."
- "with . . . trusted third parties, to ensure that you have a safe, high-performance experience”

PROTECTING MOBILE DEVICES

Mobile Phones & Tablets

Key concepts for organizations

- Need to maintain consumer, retail, and financial confidence. This will reduce costs, enhance trust in the system, facilitate growth, and foster convenience.
- Organizations engaging in m-Commerce need to continue to monitor fraudulent conduct and breaches.
- Although multiple players are involved in the transaction, there needs to be standard protocol for responding to fraud.
- Banks and financial institutions need to constantly monitor, evaluate and adjust to new threats as well. Online banking requires an institution to be able to download upgrades, patches, and changes to its mobile banking produce which the customer must install to continue using the product.

Key concepts for users

- Consumers need to pay attention to their credit card statements to check that you are paying for what they actually purchased.
- Stick to known app stores. Malware and other security threats arise most often from third party apps. Download mobile payment applications from a reputable app store. Check user reviews of the app and make sure to read app’s privacy policy on what data of yours it is accessing and sharing.
- Mobile users need to take additional protections including remote locking and wiping (less than half of users have this feature) as well as data encryption (about 35% have this).
- Users shouldn’t conduct any mobile transactions over unsecured Wi-Fi connection. It’s much more secure to use your mobile data network.
- Users should keep their mobile software current. This includes the latest updates for any operating system, mobile browser and mobile security software.

Other tips for users

- Rather than searching for your bank’s website, type in the correct address to avoid running into any phony sites, or use your bank’s official app.
- Always password protect your device and set it to auto-lock after a certain period of time to increase your mobile security.
- Never leave your tablet unattended in a public place.
- Don’t click on links on emails and text messages from people you don’t know.
- Even if you know the company or person, use a browser to search for a link or use the company’s official app to navigate to the site.
- Always double-check the web address of a site when doing a search on your mobile phone.
- If you use online banking and shopping sites, always log out and don’t select the “remember me” function.
- Before downloading a third-party app, check other users’ reviews to see if it is safe, and read the app’s privacy policy to make sure that it is not sharing your personal information.
- Use comprehensive mobile security.

Governmental Regulations?

The participation of so many different types of companies poses a substantial challenge to regulators.

Some of the industries involved such as banks are subject to rigorous regulation, others to little or none; some are governed by federal regulations, some by state regulations.
Governmental Regulations

- The Electronic Funds Transfer Act (EFTA) and the Federal Reserve Board's Regulation E likely apply to mobile financial services. However, they provide only limited protection. The consumer's liability increases if he or she delays in notifying the financial institution.

- EFTA enacted well before invention of mobile phones and only applies if transfer is pursuant to a plan contemplating periodic or recurring transfers. Does a transfer via mobile phones qualify?

- Federal Reserve Board’s Regulation E
  - Companies not regarded as “financial institutions” are increasingly becoming involved in m-Commerce. These institutions claim they don’t have to investigate their records when a customer complains about an error. Other companies bypass “financial institutions.”
  - In these cases, the only recourse is arbitration or litigation pursuant to state law (fraud and misrepresentation).