EDUCATION

Mobile Banking Overview (NA)

JANUARY 2009

mma mobile marketing association

1.0 Introduction

The MMA's Mobile Banking Overview provides banks, savings and loans, and other financial institutions with an overview of this sector's opportunities and attributes, including market size, consumer-focused mobile banking products and services, and the mobile media channels available to them today. It also provides considerations for optimizing mobile banking communications and campaign effectiveness within each channel.

This overview is a result of ongoing collaboration between MMA member companies and the MMA North America Mobile Banking Sub-Committee of the MMA Global Mobile Commerce Committee. Committee members are representative of all parts of the mobile ecosystem, including financial institutions, wireless operators and technology enablers.

Market Size and Growth Trends

The mobile banking market has grown significantly over the past several years, particularly in the United States, where many financial institutions now offer some form of mobile services for their customers.

According to a January 2008 eMarketer article, "More flip-phones and clamshells will become portable ATMs this year, according to research firm Celent. Celent said that 10% [of all] online banking U.S. households will use mobile banking by the end of 2008. The company said that about 46 million households currently bank online. A projected 30% of U.S. households overall will bank using their mobile phones in 2010."

This trend contributes towards the anticipated growth of mobile financial information services, funds transfer, bill payment and presentation, account management and customer service solutions. It is always difficult to predict adoption rates of new services and technologies, however in this case, it is beneficial to use the adoption of online banking as a comparative measuring stick.

Although more U.S. consumers currently use PCs rather than mobile phones for banking, Figure 1 shows this gap narrowing. It is reasonable to assume based on Figure 1, that the adoption rate of mobile banking in the U.S. will follow the adoption rate of online banking. The following chart has been extrapolated from an Online Banking Report that compares the ramp-up period for online banking to the estimated ramp-up for mobile banking. It took approximately ten years (1996 – 2006) to reach 40 million online banking users. According to the OnLine Banking report, it is expected to take 10 years to reach a similar penetration rate for mobile banking.

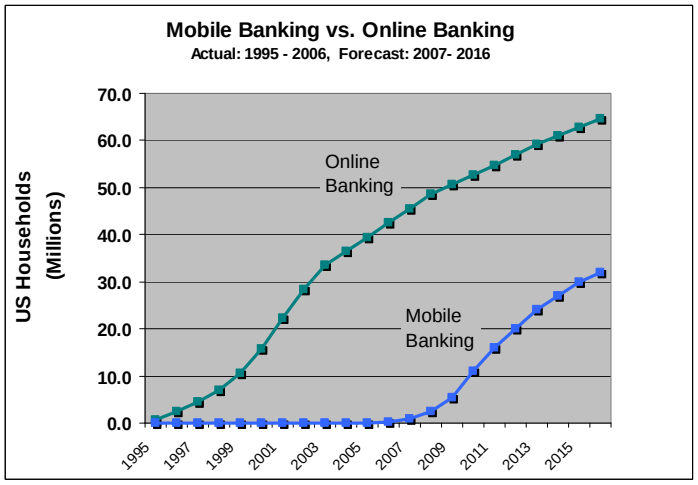

Figure 1: Mobile Banking vs. Online Banking Forecast: 1995 through 2016

U.S. households using a mobile device for banking*

Source: OnLine Banking Report, projections based on industry data, Feb 2007; accuracy estimated at +/- 25%

2.0 Mobile Banking Services

Today, most large U.S. banks offer a basic mobile banking solution for their consumers. The most common services available today are:

- Account alerts, security alerts and reminders
- Account balances, updates and history
- Customer service via mobile
- Branch or ATM location information
- Bill pay (i.e. electric bill), deliver online payments by secure agents and mobile client applications
- Funds transfers
- Transaction verification
- Mortgage alerts

Future services likely will include mobile commerce, mobile payments, contactless payments using NFC (Near Field Communications), mobile coupons and location-based services.

3.0 Mobile Channel Platforms

In creating a mobile banking solution, U.S. financial institutions use a variety of mobile media channels including Short Message Service (SMS), mobile web, and mobile client applications. Each mobile media channel has its strengths and weaknesses, and it is important to identify the delivery mode that is most appropriate for each banking service. One of the goals of this document is to provide an understanding of the

type of information that can be delivered across each mobile media channel given their strengths and limitations. As yet, no common standard for mobile services has been developed among national and/or global banks. As banking customers rapidly respond to mobile banking solutions, it will be beneficial for banks to work collaboratively to develop mobile banking guidelines at national and global levels.

Each bank must decide which and how many delivery modes it wants to offer in its mobile banking service. Most banks typically deploy a phased approach when implementing a mobile banking solution. They usually start with simple SMS alerts and notifications because these are very similar to the email alerts that they are already sending to their customers. Then they may progress to mobile web and mobile client applications. Each delivery mode has its advantages and disadvantages, which are discussed later in this section. Figure 2 provides a comparative overview of the various delivery modes:

Delivery Type	Ubiquity	Ease of Use UI	Affordability	Security	Rich Applications
SMS	●	●	●	◔	○
Mobile Web	◑	◑	◑	◑	◕
Mobile Client Application	○	◕	◑	●	●
Hybrids					
SMS with Mobile Web	◑	◕	◑	◑	◕
Secure SMS	◔	◕	◕	●	●

● Strong ◕ Good ◑ Moderate ◔ Weak ○ Poor

Figure 2: Comparative Overview of Mobile Channel Platforms

As an example, using Figure 2 data, note that SMS is ubiquitous and easy-to-use but has limited support for rich media. SMS is an ideal medium for alerts, notifications and customer-focused transactions. Mobile web, meanwhile, provides a richer experience but lacks the enormous installed base of handsets and networked users associated with SMS. Mobile client applications provide the best user experience and most security, but require users to download an application to their phone.

Therefore, it seems logical to combine wireless mediums to offer the most robust offer to the consumer. For example, a client application supporting a rich feature set for performing sensitive operations, enhanced with SMS for notification and status, without disclosing privacy-related information, is an option for banks to consider.

3.1 Short Message Service (SMS)

3.1.1 Summary

The majority of mobile phones sold in the U.S support SMS, so this technology provides financial institutions with a way to serve the widest possible market. From a consumer's perspective, SMS is also relatively inexpensive compared to other data services. These are among the reasons why many Tier 1 banks – both in the U.S. and abroad – have already deployed some form of SMS-based mobile banking service. SMS can also be used in conjunction with other delivery modes, such as mobile web (These hybrid modes are discussed later in this section.)

A simple application or set of APIs can be used by a bank to generate short messages to send to a customer's mobile device, or respond to a customer's request. For example, a user generates and sends a request SMS to a bank to request information (e.g. ATM location). The appropriate information is then returned via an SMS reply. SMS messages on most operators can be up to 160 characters in length[1].

A shortcode is a 5 or 6 digit number that is licensed by a company for use in their mobile service. For example, a bank would license a short code that they would use to communicate with their customers for an SMS mobile banking service. A short code is similar to a company's URL – a unique locator for communication between a company and their customers. For more information, refer to: http://mmaglobal.com/shortcodeprimer.pdf.

Figure 3 shows an example of an SMS mobile banking notification.:

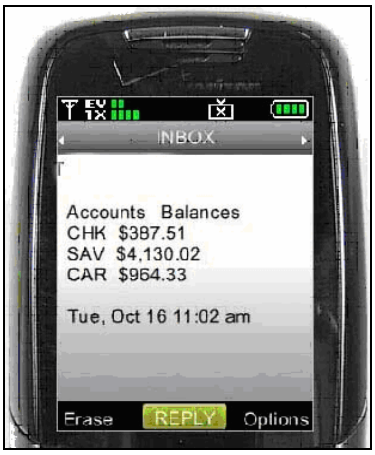

Figure 3: Mobile Banking Notification

[1] Some wireless operators restrict the SMS message to 140 characters.

3.1.2 Advantages & Disadvantages

SMS has a variety of advantages and disadvantages for financial applications and services:

Advantages

- Easy-to-use
- Common messaging tool among consumers
- Works across all wireless operators
- Affordable for consumers
- Requires no software installation
- Allows banks and financial institutions to provide real-time information to customers and employees
- Stored messages can be accessed without a network connection

Disadvantages

- Text-only and limited to 140-160 characters per message
- Does not offer a secure environment

3.1.3 Technical Implementation

In order to implement an SMS service, financial institutions may choose to work with an SMS aggregator or a technology enabler, who will ensure that the needed connections to each wireless carrier's SMS gateways are established in order to deliver messages reliably. The MMA recommends that financial institutions verify that the chosen partner is capable of providing the level of service and support necessary for a successful implementation.

Aggregators provide a set of industry-standard Application Programming Interfaces (APIs) that financial institutions use to send messages to them for delivery to customers. Aggregators typically support HTTP, SMPP and Web Services.

Figure 4 provides a high-level overview of the message flow for an SMS-based banking service.

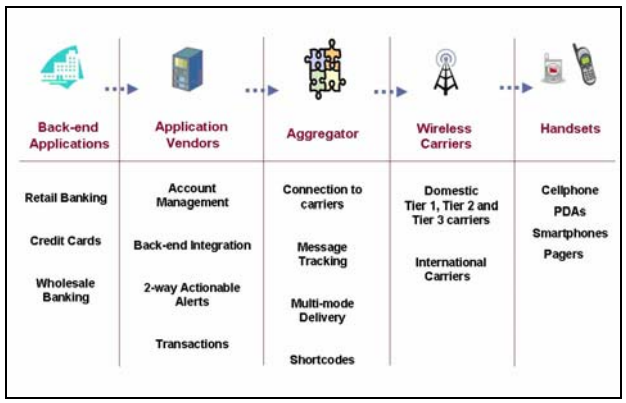

Figure 4: SMS Message Flow

3.2 Mobile Web

3.2.1 Summary

Many mobile phones sold in the U.S. market over the last five years include a web browser which provides access to the internet. At the same time, the rate plans for web browsing have become more affordable, handset screens have become larger with higher resolution, and mobile networks have upgraded to broadband speeds. This combination of affordability and steadily improving user experiences are encouraging more consumers to use their phone's browser on a regular basis.

The mobile web is comparable to the fixed internet circa 1997 when there was still confusion over browsers (Netscape vs. Microsoft) and a wide range of access speeds from dial-up to broadband. Companies had to spend time and energy to produce versions of their websites to address these variables.

Today, the mobile web poses issues that include a variety of mobile browsers, screen sizes as well as a wide range of access speeds (2G, 3G, WiFi). There are a host of companies who can provide assistance in adapting existing websites for mobile handsets and the MMA is working to establish guidelines and best practices to ensure consistency and continuity across devices as well as a high quality of experience for the consumer.

The mobile web allows users to access web sites from their handset. The mobile web is a channel for delivery of web content, which offers and formats content to users in awareness of the mobile context. The mobile context is characterized by the nature of personal user information needs (e.g. updating a blog, accessing travel information, receiving news update), constraints of mobile phones (i.e. screen size, keypad input) and special capabilities (i.e. location, connection type such as 3G or WLAN). Mobile web sites include the well-known .com domain and .mobi, which was created by a consortium of companies including Google, Microsoft, Nokia, Samsung and Vodafone.

The mobile web also includes the Wireless Application Protocol (WAP), which is an open standard to enable access to the internet from a mobile device.

Although the mobile web suffers from the proliferation of many different browsers on devices with various form factors, the majority of the handsets available today come with a browser.

On the top of the fragmented technology landscape, online banking practitioners should be aware of a couple of concepts which illustrate the current trend of mobile web browsing on mobile devices: "on-portal browsing" and "full-browsing". The "on-portal browsing" is the original mobile web content distribution model on handsets. With the "on-portal browsing", users find content via carriers' portals on handsets. Alternatively, users can go to a URL to visit a mobile web site

("off-portal"). Most carriers allow "off-portal" browsing today. "Full-browsing" is an effort to allow mobile device users to browse desktop web sites on small screens. "Full-browsing" capability is limited to selected devices and still comes with technical and usability constraints. The quality of the "full-browsing" experience on mobile devices today varies significantly depending on the design and the structure of the desktop web site.

3.2.2 Advantages & Disadvantages

The mobile web has a variety of advantages and disadvantages for financial applications and services:

Advantages

- User experience of browsing the internet from a mobile device is familiar and offers a rich UI experience
- Allows end users to access corporate applications
- Secure connection can be established on most of the mobile browsers

Disadvantages

- Many non-standard variables including handsets, browsers and operating systems
- Inconsistent user experience due to varying connection speeds and handset limitations
- User needs to have a data plan, which may be a barrier to adoption among price-sensitive demographics
- No "off-line" (out of the coverage) capability

3.2.3 Technical Implementation

The mobile web uses XHTML, a successor to HTML, developed to address the need to deliver content to devices other than desktop computers. Smart phones are devices that have a large screen and a keyboard and are more suited for accessing the mobile web. In comparison, most smaller mobile phones do not have the resources necessary to support a good mobile web experience or the additional complexity of standard HTML syntax. XHTML provides an alternative to standard HTML syntax, whose complexity is more than most mobile phones can handle. XHTML can be thought of as the intersection of HTML and XML in many respects because it is a reformulation of HTML in XML. XHTML 1.0 became a World Wide Web Consortium (W3C) recommendation on January 26, 2000. XHTML 1.1 became a W3C recommendation on May 31, 2001. As a result, XHTML has had years to develop a following among handset vendors, application developers and other key players. For more information about XHTML, visit:

http://www.w3.org/TR/xhtml1.

3.3 Mobile Client Applications

3.3.1 Summary

U.S. financial institutions and their customers are increasingly adopting advanced agent-based technologies and other downloadable applications. These technological advancements in handsets will introduce and create a more secure, user-friendly environment with many rich features for both banks and their customer base. However, there are still many issues that need to be overcome before downloading applications to handsets becomes as ubiquitous as alternatives such as SMS.

Mobile client applications are a rapidly developing segment of the global mobile market. Mobile client applications (a.k.a. downloadables, client applications) are common on most mobile phones today and are key to providing user interfaces for basic telephony and messaging services, as well as for more advanced and entertaining experiences such as playing games, browsing and watching videos on mobile phones.

Mobile client applications have evolved to give a user access to services that require richer, faster and not necessarily connected user experiences. In this respect, mobile applications are distinctly different from browsing the mobile web (albeit there are some emerging trends around JavaScript/ AJAX and mobile widgets which will cross over between both worlds).

The combination of a client application on the handset and a server component enables many benefits including the access to all banking functionalities, strong authentication and encryption of sensitive data, and the ability for customization and branding. If a full client is not required, a lightweight encryption technology could enable mobile banking deployments on devices not supporting rich clients, or simply whenever managing and pushing such applications is not possible.

From a technical point of view, mobile client applications are differentiated by the runtime environment in which they are executed:

- Native platforms and operating systems, such as Symbian, Blackberry Windows Mobile and Linux
- Mobile web/browser runtimes, such as Webkit, Mozilla/Firefox, Opera Mini and RIM
- Other managed platforms and virtual machines, such as Java/J2ME, BREW, Flash Lite and Silverlight

Mobile client applications can offer powerful and secure application functionality while protecting the consumer and the application data on the mobile handset. Once installed and configured on the mobile handset, the application vendor can

easily distribute updates, upgrades, and easily manage the device and application configuration.

Figure 4 shows sample screen shots of a mobile banking client:

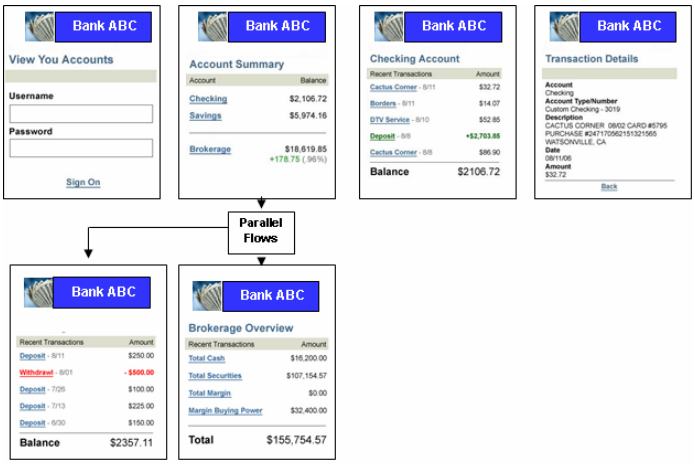

Figure 4: Mobile Banking Client

3.3.2 Advantages & Disadvantages

Mobile client applications have a variety of advantages and disadvantages for financial applications and services:

Advantages

- Offers organizations more control over the user experience, with a rich user interface capability
- Ability to work even when there is no connection to the wireless network
- Secure access can be established with applications
- Support for access to corporate or custom applications
- Most applications also provide the ability to provide remote wipe-out of information when device is lost or stolen

Disadvantages

- Thousands of different combinations for devices, operating systems and development environments may prevent support for all devices
- Differing handset capabilities and performance causes inconsistent user experience when using or downloading an application
- Possible increase in customer service and support issues

Perhaps the most challenging part of the client application is the deployment of the application to the mobile handset. Not all handsets have similar screen sizes, user interfaces or operating systems. For example, with more than 12,000 different handset models already in use worldwide, creating, deploying and supporting new software on mobile phones is an arduous task. There are currently seven different major smartphone operating systems (i.e., Windows Mobile, BlackBerry, Palm, Symbian, Linux, iPhone and Android), hundreds of feature phone operating systems known as real-time operating systems (RTOSs), six different major application development environments (BREW, J2ME, Symbian, Android, Blueprint, iPhone SDK), more than 130 different hardware platforms and a multitude of differences between GSM and CDMA networks. The fundamental difficulties of developing applications to accommodate all of these mobile phone variations make widespread availability to all customers extremely difficult.

To add to the confusion, most wireless operators provide a wide range of handsets that cover all of the operating systems listed above. In addition, J2ME and Symbian development environments are supported on most wireless operators, while some U.S. carriers support only BREW applications.

3.3.3 Technical Implementation

Java 2 Micro Edition (J2ME), offered by Sun Microsystems, Inc, enables developers to quickly develop mobile applications solutions. Sun designed J2ME to allow experienced Java programmers and developers to rapidly develop and deploy mobile applications.

While using a development platform based upon a mature language substantially lowers the learning curve for developers, the platform is susceptible to at least some of the security issues of the base platform.

Java has become a standard dominant language for server-side programming. Java makes it easier to write safe, reliable code through features, such as automatic memory management and structured exception-handling. A large set of APIs and cross-platform design provide power and portability. Sun has announced significant enhancements for mobile computing and interfaces to wireless networks. Several application servers support Java interfaces.

Binary Runtime Environment for Wireless (BREW), is a Qualcomm-developed open-source application development platform for wireless devices. It enables developers to create portable applications that work on any mobile phone supported by the CDMA Development Group. This support includes SMS, e-mail, location positioning, games and internet radio applications.

3.4 SMS with Mobile Web

3.4.1 Summary

An SMS message with an embedded URL (aka: WAP Push) allows a user to easily connect to a specific mobile web page by clicking on the URL link. This approach combines the immediacy of SMS with the richer experience of the mobile web. For example, an SMS alert can be sent to a user with a notification that there has been a charge on the user's credit card, and direct the user to click on the embedded link to receive more information.

Figure 5 shows an example:

Figure 5: SMS with WAP Push

3.4.2 Advantages & Disadvantages

SMS with WAP Push has a variety of advantages and disadvantages for financial applications and services:

Advantages

- The majority of US wireless carrier networks allow a user to click on an embedded URL (WAP Push) in the SMS message and go directly to their desired web page
- Secure connection can be established on most of the mobile browsers

Disadvantages

- User must have a data plan that includes SMS and web access
- Some wireless operators do not support clickable WAP links in SMS messages
- No "off-line" (out of the coverage) capability

3.4.3 Technical Implementation

The implementation of a WAP Push service is a combination of working with an SMS partner, and developing a mobile web landing page.

3.5 Secure SMS

3.5.1 Summary

Secure SMS combines a mobile client application with SMS to leverage the personalized messages and real time alerts associated with SMS while increasing security and expanding functionality. Secure SMS exchanges encrypted messages via SMS. The Secure SMS messages trigger SMS notification, offer an expanded character limit from 160 to 5000 characters, and are stored in a secure application that can be protected with a customers' PIN. This allows the transmission of sensitive information, such as customer's private data, user-ids, passwords and transaction information to be kept private.

Figure 6 shows an example of Secure SMS:

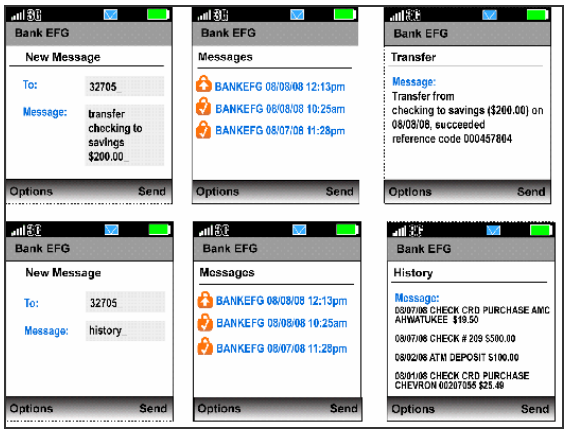

Figure 6: Secure SMS

3.5.2 Advantages & Disadvantages

Secure SMS has a variety of advantages and disadvantages for financial applications and services:

Advantages

- Secure, end-to-end encryption of SMS, and secure access can be established with applications
- Allows organization to provide real-time information to customers and employees
- Stored messages can be accessed without a network connection
- Remote data wipe in case of loss or unauthorized access attempts
- Message size can be up to 5000 characters
- Similar interface as consumer based SMS which is common messaging tool among consumers
- Allowing access to corporate or custom applications

Disadvantages

- Thousands of different combinations for devices, operating systems and development environments may prevent support for all devices.
- Differing handset capabilities and performance causes inconsistent user experience when using or downloading an application
- Possible increase in customer service and support issues

3.5.3 Technical Implementation

A simple mobile application needs to be installed on the handset but no data plan is required. An application or set of APIs can be used by the bank to generate short messages and have them delivered to their customers' mobile devices. One could send a request SSMS (as a mobile originated or MO-SM) to the bank and obtain the specific password (as a mobile terminated message: MT-SM) in a SSMS reply.

4.0 Security

Users will expect at least the same level of security that's available when banking online via their PC. Both the real problem (e.g., eavesdropping, injection and modification) and the "perception" issue (e.g., how security – or lack thereof – affects the financial institution's brand) must be addressed in order to encourage adoption of mobile banking.

Data transmission must be secure: In this case, the term "secure" addresses mainly the concept of confidentiality and therefore requires encryption of the connection between the device and the bank.

Application and data access must be controlled: Before users can receive any sensitive information related to their bank accounts, a certain degree of verification must be completed. Ideally, the combination of several authentication factors and the possibility to challenge the user in case of a (potential) security breach should be part of the procedure.

Data integrity must be provided: Any critical data stored on the mobile device must be protected against unauthorized modification. The issue of possible corruption and deletion error of sensitive information should also be addressed.

Loss of device must have limited impact: The mobile banking service should be designed so that there's limited impact when customers lose their handsets. For example, the service could support a remote-locking feature embedded in the software client that prevents a lost phone from accessing the customer's account. Such features also provide the peace of mind that helps encourage customers to try mobile banking.

4.1 Security Measures by Mobile Channel

Each mobile channel offers its own strengths with respect to security, but there are other ways financial institutions can enhance security in each mobile channel.

4.1.1 SMS Security

A financial institution should be mindful that SMS is not considered secure. SMS requires the addition of full encryption, both on the handset and over the air in order to guarantee the same level of security as a mobile client application or the mobile web. SMS security is particularly important whenever a device is lost or stolen, since SMS can be accessed without authorization.

To eliminate security risks, personal information can be sent using a hybrid solution: SMS with mobile web (aka: WAP Push), or Secure SMS. Alternatively, the bank may call customers to verify their identity before providing personal information.

The SMS gateway also should be secured to prevent unauthorized access. Recommendations for securing the facility that houses the gateway include:

- 24-hour security guards and multiple tiers (doors) of access to inner areas
- Access control systems including biometrics in addition to magnetic badges
- Logging of all accesses for audit purposes
- Motion and infrared sensors in sensitive areas
- Secure cabinets and hardware for all cryptographic storage
- Additionally, trusted employees (i.e. employees having undergone an in-depth secure background check) are usually the only personnel authorized in sensitive areas

4.1.2 Mobile web Banking

Secure banking on the mobile web is similar to PC-centric banking services that use https. The mobile web limits storage risks and can use secure communication to eliminate eavesdropping and data alteration risks.

4.1.3 Mobile Client Application

Mobile client applications are a more secure channel for transmission of data because the combination of a client application on the handset and a server allow for strong authentication and encryption of sensitive data. The transmission of sensitive information, such as customer's

private data, user IDs, passwords and transaction information must be kept private.

However, mobile client applications are at risk of malware attacking the client application on the device. This – currently limited - risk can be mitigated by adding virus and trojan detection at different system layers, for example: controlling/filtering application and content delivery, and adding virus scan and trojan detection on the handset.

4.2 Mobile Network Operator Security

4.2.1 GSM Network Security

GSM security algorithms are used to provide authentication and radio link privacy to users on a GSM network. GSM uses three different security algorithms called A3, A5, and A8. In practice, A3 and A8 are generally implemented together (known as A3/A8).

An A3/A8 algorithm is implemented in Subscriber Identity Module (SIM) cards and in GSM network Authentication Centers. It is used to authenticate the customer and generate a key for encrypting voice and data traffic, as defined in 3GPP TS 43.020 (03.20 before Rel-4).

An A5 encryption algorithm scrambles the user's voice and data traffic between the handset and the base station to provide privacy. An A5 algorithm is implemented in both the handset and the base station subsystem (BSS).

In recent years, several attacks have been identified. Given improvements to cryptographic algorithms and network equipments, for an attack to succeed, it would have to be an active one; requiring the attacker to transmit distinctive data over the air to masquerade as a GSM base station. An attacker would also have to physically stand between the caller and the base station to intercept the call. Obviously, transmitting on an operator's radio frequencies is illegal in most countries, though the threat scenario exists.

4.2.2 CDMA Network Security

CDMA uses specific spreading sequences and pseudo-random codes for the forward link (i.e. the path from the base station to the mobile) and on the reverse link (i.e. the path from the mobile to the base station). These spreading techniques are used to form unique code channels for individual users in both directions of the communication channel. Because the signals of all calls in a coverage area are spread over the entire bandwidth, it creates a noise-like appearance to other mobiles or detectors in the network as a form of disguise, making the signal of any one call difficult to distinguish and decode.

CDMA also has a unique soft handoff capability that allows a mobile to connect to as many as six radios in the network, each with its own Walsh code. Due to this architecture, someone attempting to eavesdrop on a subscriber's call has to have several devices connected at exactly the same time in an attempt to synchronize with the intended signal. In addition, CDMA employs a fast power control - 800 times per second- to maintain its radio link. It is difficult for a third party to have a stable link for interception of a CDMA voice channel, even with a full knowledge of a Walsh code. Synchronization is critical, as without this synchronization, the listener only hears noise.

Subscriber authentication is a key control mechanism to protect the infrastructure and to prevent unauthorized access to network resources. Access authentication is accomplished by means of an 18-bit authentication signature that is verified by the network's databases of user information, the Home Location Register (HLR) and Authentication Center.

4.3 Potential Threats

Financial institutions should be aware of the types of potential threats that can affect their mobile banking services. These include:

Cloning – Copying the identity of one mobile phone to another, thereby allowing the perpetrator to masquerade as the victim, normally with the intent to have calls and other services billed to the victim's cellular account. In the case of mobile banking, cloning could give the hacker access to the victim's financial accounts.

Hijacking – The attacker takes control of a communication between two entities, masquerading as one of them. As with cloning, hijacking could give the hacker access to the victim's financial accounts.

Malicious Code – Software in the form of a virus, worm or other "malware" is loaded onto the handset, the SMS gateway or the bank's server to perform an unauthorized process that will have adverse impact on the confidentiality, integrity or availability of financial information and transactions.

Malware – A contraction for "malicious software" that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim's data, applications or operating system, or otherwise annoying or disrupting the victim.

Man-in-the-Middle Attack – An attack on the authentication protocol exchange in which the attacker positions himself between the claimant and verifier with the intent to intercept and alter data traveling between them.

Phishing – Tricking a victim into disclosing sensitive personal information or downloading malware through an email.

Redirecting – Intercepting a communication by substituting a fraudulent address or identity, potentially by using a Man-in-the-Middle attack.

SMiShing – A contraction of "SMS phishing," this attack uses SMS to facilitate bogus requests for personal information.

Spoofing – Sending a network packet that appears to come from a legitimate source, rather than its actual source.

Vishing – A contraction of "voice and phishing", in which victims are tricked into disclosing sensitive personal information through a phone call.

5.0 General Conduct

The MMA recommends that all mobile banking campaigns comply with the applicable MMA guidelines, including but not limited to the Global Code of Conduct, U.S. Consumer Best Practice Guidelines and the Global Mobile Advertising Guidelines. All of these documents are available as free downloads at http://www.mmaglobal.com/policies.

5.1 Federal and State Regulations

At all times, programs must be in accordance with applicable federal and state laws, rules and regulations. Additionally, all mobile banking services must comply with federal and state banking guidelines, such as those put in place by the Federal Reserve System, Federal Deposit Insurance Corporation and National Credit Union Administration.

CAN-SPAM regulations apply to email marketing and explicit opt-in must be conducted prior to email remarketing.

5.2 Consumer Information

A financial institution should use the same security precautions for mobile services as they use for their other communication channels like email. For example, they should inform their customers that they will never request PIN or other sensitive information over the mobile channel. Please refer to Figure 2 in Section 4 to determine the relative levels of security for each of the mobile delivery channels.

5.3 Customer Service

A financial institution should provide the same access to customer support for the mobile channel as they do for their more traditional communication channels. Please refer to the MMA Consumer Best Practices Guidelines for more information on acceptable practices in the United States.

6.0 Who We Are

About the Mobile Marketing Association

The Mobile Marketing Association (MMA) is the premier global non-profit trade association established to lead the growth of mobile marketing and its associated technologies. The MMA is an action-oriented organization designed to clear obstacles to market development, establish mobile media guidelines and best practices for sustainable growth, and evangelize the use of the mobile channel. The more than 700 member companies, representing over forty countries around the globe, include all members of the mobile media ecosystem. The Mobile Marketing Association's global headquarters are located in the United States and it has regional chapters including North America (NA), Europe (EUR), Latin America (LATAM), Middle East & Africa (MEA) and Asia Pacific (APAC) branches. For more information, please visit www.mmaglobal.com.

About the MMA Mobile Banking Sub-Committee

The MMA Mobile Banking Sub-Committee has been established to advance the mutual interests of financial institutions, wireless operators, and technology providers to promote mobile banking and remove obstacles for growth. By creating overviews and guidelines agreed upon by wireless operators, financial institutions and technology providers addressing the major issues of any mobile banking service, our goal is to ensure a consistent, secure and user-friendly mobile banking experience and provide banks with a reliable source of information from which to base their decisions. The Mobile Banking Sub-Committee is part of the MMA Global Mobile Commerce Committee.

The MMA Mobile Banking Sub-Committee, chaired by CellTrust and VeriSign, Inc., developed these guidelines in collaboration with the following MMA member companies:

MMA North America Mobile Banking Sub-Committee		
Acuity Mobile	Silverback Media	Virgin Mobile, USA
AT&T Mobility	Sprint	Washington State Employees Credit Union
CellTrust Corporation	VeriSign, Inc.	
Fidelity Investments	Verizon Wireless	

7.0 References

The following links provide additional sources of information and reference:

- MMA U.S. Global Code of Conduct
  http://www.mmaglobal.com/codeofconduct.pdf
- MMA Global Consumer Best Practices Guidelines
  http://www.mmaglobal.com/bestpractices.pdf
- Mobile Marketing Association Website
  http://www.mmaglobal.com
- MMA Mobile Advertising Guidelines
  http://www.mmaglobal.com/mobileadvertising.pdf
- Mobile Applications
  http://www.mmaglobal.com/mobileapplications.pdf
- Mobile Measurement Ad Currency Definitions
  http://www.mmaglobal.com/adcurrencies.pdf
- Understanding Mobile Marketing: Technology & Reach
  http://www.mmaglobal.com/uploads/MMAMobileMarketing102.pdf
- Off Portal – An Introduction to the Market Opportunity
  http://www.mmaglobal.com/offportal.pdf
- Mobile Marketing Sweepstakes & Promotions Guide
  http://www.mmaglobal.com/mobilepromotions.pdf
- Mobile Search Use Cases
  http://www.mmaglobal.com/mobilesearchusecases.pdf
- Introduction to Mobile Coupons
  http://www.mmaglobal.com/mobilecoupons.pdf
- Introduction to Mobile Search
  http://www.mmaglobal.com/mobilesearchintro.pdf
- Short Code Primer
  http://www.mmaglobal.com/shortcodeprimer.pdf
- W3C Mobile Web Best Practices
  http://www.w3.org/TR/mobile-bp/
- W3C mobileOK Basic 1.0 Guidelines
  http://www.w3.org/TR/mobileOK-basic10-tests/
- W3C mobileOK Checker

  http://validator.w3.org/mobile

8.0 Contact Us

For more information, please contact:

Mobile Marketing Association

Email: mma@mmaglobal.com

www.mmaglobal.com

9.0 Glossary of Terms

The MMA maintains a nomenclature glossary of all terms within MMA guidelines, education documents and research. The glossary is available at:

http://www.mmaglobal.com/glossary.pdf.

The Mobile Marketing Association is the premier global organization that strives to stimulate the growth of mobile marketing and its associated technologies. The MMA is a global organization with over 700 members representing over forty countries. MMA members include agencies, brands, content providers, hand held device manufacturers, operators, technology enablers, market research firms, as well as any company focused on the potential of marketing via mobile devices.