CTIA
The Wireless Association®

Best Practices and Guidelines

for

Mobile Financial Services

Version 01.14.2009

Effective Date: January 28, 2009

CTIA
The Wireless Association®

TABLE OF CONTENTS

Section 1 - Purpose

Mobile financial services ("MFS"), such as mobile banking, mobile payments and mobile commerce, represent a growing and promising class of mobile services for consumers. CTIA, in association with the leading U.S. wireless carriers, has developed these Best Practices and Guidelines ("Guidelines") to promote clear and rewarding consumer experiences, to establish an environment where MFS transactions are authorized, secure, and compliant with applicable laws and industry guidelines, and to protect user privacy and financial data.

Section 2 - Applicability

These Guidelines apply to MFS Providers. MFS Providers are the parties that provide MFS to mobile users or provide back-end services supporting MFS transactions. Wireless carriers can be MFS Providers in certain circumstances, but do not constitute MFS Providers for purposes of these Guidelines merely because they provide wireless data services, application provisioning services, or similar standard functions to mobile users and MFS Providers.

Examples of MFS Providers:

1) A financial institution that provides its banking, brokerage or other financial services (e.g., account balance inquiry, bill payment) via the mobile channel is an MFS Provider.

2) A software developer or platform provider that develops and/or supports mobile banking or mobile payment services on behalf of financial institutions is an MFS Provider.

3) A provider of an online payment service (e.g., online commerce, bill payment, person-to-person transfer) that provides such services via the mobile channel is an MFS Provider.

4) A payment card issuer or payment network that provides credit cards, debit cards, stored value cards, or transit fare intended to be provisioned to mobile handsets is an MFS Provider.

5) A provider of an application for mobile parking meter payments is an MFS Provider.

6) A mobile commerce service provider that enables (through short codes or direct relationships) billing of physical goods to the user's monthly wireless statement is an MFS Provider.

7) A wireless carrier that provides to consumers its own MFS under its own brand is an MFS Provider.

Providing digital goods that are directly associated with mobile phone service, or providing a payment service for such digital goods, does not make a wireless carrier an MFS Provider.

Providing payment services for mobile phone services does not make a wireless carrier an MFS Provider.

Caveats: (a) The examples are illustrative only and do not imply that compliance with the Guidelines alone is sufficient to provide MFS. (b) The business terms applicable to any particular MFS are beyond the scope of these Guidelines.

Section 3 – Guidelines

A. Guidelines Specific to Mobile Banking and Mobile Payments

1. Authentication and Authorization

MFS Providers should use methods consistent with industry best practices to authenticate user identity and obtain user authorization for mobile banking and mobile payment transactions.

Examples of industry best practices may include multifactor authentication, PINs, shared secrets, challenge questions, one-time use passwords and codes, and express authorization of transactions.

2. Banking and Payment Alerts; Transaction Records

MFS Providers should provide controls that allow users the ability to receive banking and payment alerts and notices in accordance with user preference. MFS Providers should also provide systems that allow users to access transaction records and other information about their accounts.

3. Limiting Liability for Unauthorized Transactions

MFS Providers of mobile payment systems should disclose all material information regarding the liability, if any, that the user may have for unauthorized transactions or fraudulent use. MFS Providers of mobile payment systems should create policies that cap liability for unauthorized transactions. Such policies should, at a minimum, comply with liability caps required under existing legal requirements (*e.g.*, $50 or other applicable liability cap for unauthorized credit card transactions or electronic funds transfers). MFS Providers should consider incorporating into the MFS controls that limit financial risk to the consumer, such as usage caps and spending limits.

B. Guidelines Specific to Mobile Commerce

1. Disclosure of Material Terms of Purchase

MFS Providers should disclose, in a clear and conspicuous manner, the material terms of each purchase, including a description of the product or service being purchased, taxes, surcharges, and other fees, and refund policies. This may include disclosures off of the mobile device.

2. Obtaining User Authorization

MFS Providers should obtain user authorization for purchases, consistent with industry best practices.

> *Examples of industry best practices may include express authorization of transaction, confirmation screen, transaction cancellation option, and opt-in for subscription services.*

3. Receipts, Order Status and Account Information

MFS Providers should make receipts or proofs of purchase available for mobile purchases. MFS Providers should also provide systems that allow users to access order status and other information about their accounts. The appropriate methods of presenting such information (*e.g.*, via an SMS message, email, on a website, on the mobile service bill, paper receipt, etc.) and the level of information available will vary depending upon the type of service.

4. Mobile Coupons, Rebates, Loyalty Programs, etc.

MFS Providers should disclose, in a clear and conspicuous manner, the material terms of mobile coupons, rebates, loyalty programs and similar products. Such terms include redemption values, expiration dates, fees, limitations on use and other restrictions.

5. Minors

MFS Providers of age-restricted products, services or applications must include clear and conspicuous warnings and use appropriate methods of age-screening or verification before allowing purchase.

C. General Guidelines

1. Disclosure of Terms; Disclaimers

The identity of the MFS Provider and all material terms relevant to an MFS should be disclosed in a clear and conspicuous manner to users prior to their use of the service. Such disclosures should include applicable disclaimers.

> *Examples of material terms and disclaimers may include a description of the MFS, terms of use, applicable fees, purchase price, method and frequency of billing, use restrictions and limitations, liability caps, and disclaimers of liability and warranties.*

2. Consent to Enrollment in MFS

MFS Providers should obtain affirmative consent from the user for the enrollment of the user in an MFS. Notice should be given to the user that will allow the user to make an informed decision prior to taking any action that will result in the user incurring a charge (*e.g.*, a charge for text message that contains confirmation of a transaction, for data plan usage after enrollment, or to a wireless or payment account).

3. Compliance with Laws and Regulations

It is the responsibility of each MFS Provider to provide the products, services, software, and/or hardware provided by that MFS Provider in accordance with all applicable local, state, and federal laws, payment network rules, and mobile industry best practices guidelines.

> *Examples of laws, regulations and mobile industry best practices guidelines that may apply to MFS Providers include, but are not limited to: state and federal banking laws, the Electronic Funds Transfer Act, Regulation E, the Bank Secrecy Act, federal Money Services Business laws, state money transmitter laws, the Truth in Lending Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act (GLBA), state gift certificate laws, federal and state debt collection laws, NACHA - The Electronic Payments Association (NACHA) rules, Federal Financial Institution Examination Council (FFIEC)*

rules, Payment Card Industry (PCI) Security Standards Council rules, and CTIA – The Wireless Association's Best Practices and Guidelines for Location-Based Service.

4. Security of Data Transmissions

MFS Providers should utilize industry best practices when providing security of data during transmission. MFS Providers should not rely solely on GSM, CDMA or other wireless network security.

Examples of industry best practices may include encryption, hashing or compensating controls to create secured sessions.

5. Security on the Mobile Device or in Storage

MFS Providers should use industry best practices to protect against unauthorized access to MFS data on a mobile device or in other storage locations. Such protections may include mechanisms for keeping software applications separate, keeping MFS data and MFS communications secure, and protecting memory from unauthorized access or modification.

Examples of industry best practices may include PIN protection, remote device disabling or wiping, and encryption of sensitive information on the device.

6. Access Controls and Security of Sensitive Information

MFS Providers should offer access control options and tools that enable users to protect their data and to limit unauthorized party access to sensitive information on the device. MFS Providers should educate users on the importance of protecting their personal information, and how to use application security features and capabilities.

Examples of sensitive information include Social Security numbers, bank account numbers, PINs, passwords, and personally identifiable information. Personally identifiable information may include any information that could be used to create a fraudulent identity or transaction.

Examples of tools for protection of personal information may include encryption, hashing or compensating controls, and password protection.

7. Fraud and Identity Theft Protection

MFS Providers should incorporate into their MFS fraud-prevention techniques and offer tools to protect users' information, funds, credit, and identities.

> *Examples of fraud-prevention techniques and tools may include proactive user identification, detection and response to transaction/use patterns, practices or specific activities, customer ability to place limitation on spending, etc.*

8. Collection, Use, and Disclosure of Information

(a) Information Use. MFS Providers should provide clear disclosures about their access, collection, use, storage and disclosure of personally identifiable information. The MFS Provider should not access, collect, use, store or disclose the personally identifiable information for any purpose other than provision of the MFS, unless it provides appropriate notice and obtains consent from users. Such notice should explain, for example, the other intended uses (*e.g.*, the use of the information for advertising) of the information. MFS Providers that use the information collected to create aggregate data should remove or permanently obscure the consumer's identity and provide clear notice of such aggregation and use.

(b) Security Incident. In the event of a security breach, MFS Providers should notify consumers of such breach in accordance with relevant breach notification laws. MFS Providers should respond to the breach as the responsible party. Although wireless carriers are not responsible for providing notice, the MFS Provider should coordinate and collaborate with wireless carriers to ensure the wireless carriers are prepared for inquiries related to the incident. The MFS Provider should be the user's main point of contact regarding the breach, and the wireless carriers should not be referenced in any breach notice.

9. Dispute Resolution Processes and Customer Service

MFS Providers should develop reasonable dispute resolution processes for handling disputed payments and transactions. MFS Providers also should have processes in place to address general customer complaints related to the use of the MFS. MFS Providers should provide customer service via an appropriate method (phone, online, SMS, etc.) and at commercially reasonable times. Responses to inquiries should be made in a reasonably expedient manner and as appropriate for that MFS. MFS Providers should make customer service contact information readily available so that customer service requests can be properly directed.