

Text Message Mobile Marketing: Risks for ISOs, Agents, and SMBs Involved with Non-Compliant Programs

Text message marketing is a new tool for increasing sales and building customer loyalty. What many people do not know, however, is that there are industry rules and best practices governing how text message marketing is used.

This document explains what's involved in getting text message programs to consumers, the rules governing the process, and the risks involved with non-compliant campaigns. The best way to avoid potentially significant business risk is to understand the industry rules and actively address compliance requirements with text message program (content) providers.

Why Text Message Marketing?

Along with the explosive growth of text messaging for personal communication, is its rapid expansion for commercial purposes. Commonly known as "mobile marketing," and specifically "text message marketing," commercial text messaging has grown dramatically over the past few years. Properly used, text message marketing can have an immediate, positive impact on business visibility and revenue.

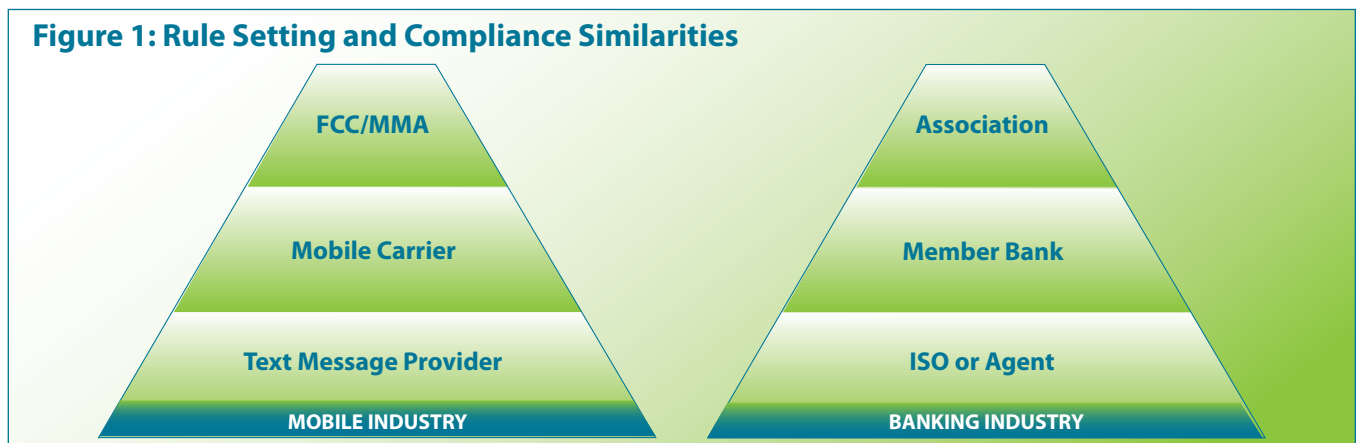
Consumers routinely read text messages within minutes of receiving them. A business can respond quickly and even automatically to market conditions, send targeted text message offers and realize an immediate, positive result. The immediacy of text message marketing is a major advantage over traditional advertising/coupon media. Additionally, if the message contains a specific offer, then the recipient doesn't have to clip and carry a coupon. The customer simply stores the offer in his phone and presents it to the merchant. Due to these factors, it's common for merchants who use text message marketing to experience much higher engagement or redemption rates than with traditional media delivery such as newspaper or mail.

Regulatory Authorities

In the mobile telephone world, the FCC and the mobile carriers have a relationship somewhat analogous to the bankcard associations and banks (Figure 1). The FCC makes and enforces the rules governing how the mobile carriers may conduct their business, just like Visa and MasterCard enforce the rules for their bank members. Like banks over Independent Sales Organizations (ISOs), the mobile carriers exercise significant compliance authority over their clients, the content providers.

Commercial text messaging is subject to the rules and standards of individual wireless carriers such as AT&T, Verizon, Sprint, and T-Mobile. The technical, structure, content, and flow guidelines for mobile marketing messages are available on each mobile carrier's developers' web site, from connection aggregators or, in consolidated form, in the Mobile Marketing Association's (MMA) Best Practices document.¹

Figure 1: Rule Setting and Compliance Similarities



¹ Mobile Marketing Association, "U.S. Consumer Best Practices Guidelines for Cross-Carrier Mobile Content - V6," March 2011, <<http://mmaglobal.com/bestpractices.pdf>>

Risk Overview

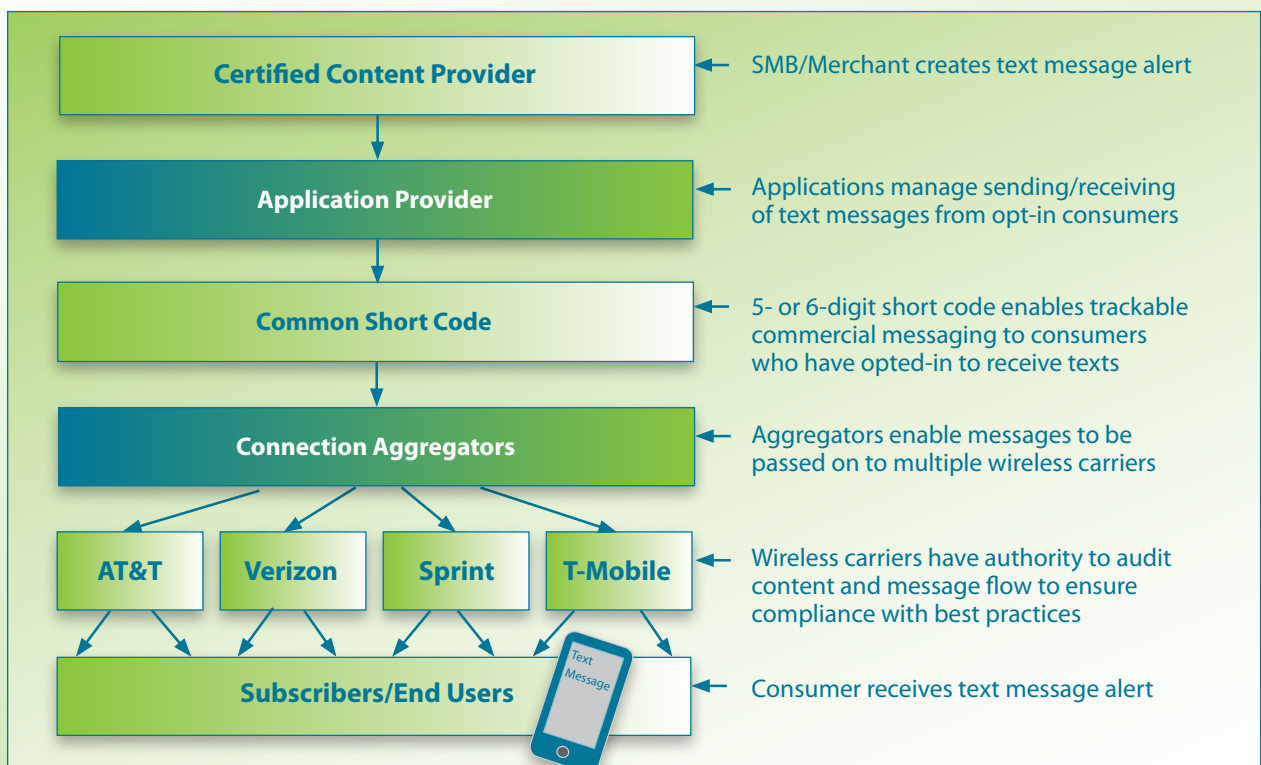
If a content provider does not comply with requirements set by the mobile carrier, the sponsor’s access to send text messages may be terminated. If the content provider’s access is terminated, all of the content provider’s customers lose their text message services. So, it is very important to fully comply with the rules.

Some entrepreneurs, ISOs, sales agents, and small to medium-sized businesses (SMBs) have aligned themselves with text message marketing companies that do not follow the published guidelines. Whether these vendors are simply unaware of the rules or intentionally choose to violate them, the result is the same. The vendor’s access to wireless customers will eventually be terminated. SMBs will lose the valuable connection with their customers. ISOs and sales agents who represent non-compliant text message marketing solutions will lose recurring revenue from merchants when carriers shut down campaigns. Entrepreneurs who paid to become “white label” text message marketing resellers will lose their investment.

How Text Message Marketing Works

The fact that text message communication is nearly instantaneous belies the number of steps and parties involved.

Figure 2: The Path of a Mobile Marketing Message



Getting a compelling text-message offer into the hands of a consumer requires several technical “handshakes” and even a possible audit by wireless carriers (Figure 2). There are two ways to send text messages to a consumer’s phone: SMTP/Email and SMS.

SMTP/Email

Some mobile carriers have an SMTP/email gateway within their network. If the carrier provides an open gateway, then

the procedure to send a message via the SMTP/Email channel is achieved by using the following syntax:

```
10DIGITMOBILEPHONENUMBER@MOBILEOPERATORSMTPEMAILDOMAIN.com
```

In the past, some companies and marketers were attracted to SMTP/Email since there is no discrete per message charge as is the case with SMS. There are two issues with SMTP/email, however. SMTP is primarily one-way communication. In addition, since the wireless carriers prohibit traffic that does not permit the user to opt out, SMTP is not compliant with MMA Best Practices or with the CAN-SPAM Act.²

Risks Associated with SMTP/Email

Wireless carriers shut down non-conforming SMTP/Email traffic when discovered. The vendor and associated businesses using the program lose connectivity with their customers. Additionally, violators may be subject to FCC action. The balance of this document focuses on SMS, the more popular method.

SMS and Common Short Codes

SMS text messages are the kind of text messages that we all know and use on our cell phones. SMS stands for Short Message Service. It allows for short text messages (160 characters) to be sent from one cell phone to another. This is the most widely used data application in the world with more than 2.5 billion users worldwide.

The wireless carriers have created a process for commercial transmission of SMS text messages to wireless consumers. To identify and track commercial text messaging, the wireless carriers created common short codes.

Short codes: A common short code (CSC), or “short code,” is a code which is common across many wireless providers. In the U.S. and Canada it is a five- or six-digit mobile number (e.g. 23456) assigned to a business that can be used for two-way SMS messaging between the business and the consumer.

A short code may be a “random” number or a “selected” number in which the business chooses the specific number (e.g. 347639 for DISNEY). Short codes protect mobile consumers from SPAM and unsolicited marketing. They identify the program sponsors to both the carriers and consumers. As mentioned, carriers may audit to ensure ongoing compliance of each short code on their networks and they can easily block programs that don’t follow their rules.

There are two types of short codes: dedicated and shared.

Dedicated short codes: A dedicated short code (Figure 2) is leased by one entity for the sole use of its certified campaign. During the lease term, the entity has exclusive use of the code. It maintains control of the code and all associated keywords.

Shared short codes: A shared short code is shared by more than one company. Since shared short codes have been provisioned ahead of time, the time to market for text message campaigns is reduced from months to weeks.

How a Short Code Works

A consumer is encouraged to send a text message to the short code by a promotion or advertising. The consumer addresses the text message to the short code and enters text, or keyword, into the message as directed (e.g. “PIZZA” keyword acknowledging they want to receive offers from a local restaurant). Keywords are alphanumeric codes that distinguish programs on a short code.

Consumers may also opt-in to receive mobile messages by entering their mobile number on a website, automatic telephone system (IVR) or upon entering their number at a Point of Sale (POS) device. In all cases, the business must follow the approved text message flow (Figure 3) that was submitted to the Common Short Code Administration (CSCA) for the business’ mobile marketing campaign.

² Federal Communication Commission, “CAN-SPAM: Unwanted Text Messages and E-Mail on Wireless Phones and Other Mobile Devices,” August 11, 2009 <<http://www.fcc.gov/cgb/consumerfacts/canspam.html>>

Figure 3 – Disclosure Excerpt From an Approved Message Flow

Opt-In Message

Consumers must ‘opt-in’ to a short code program before they can receive associated messages.

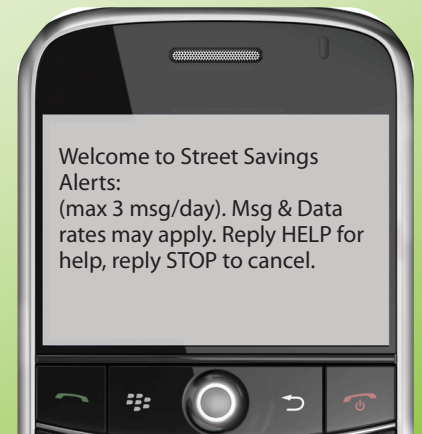
Confirmation Message

All subscription or alert programs (e.g. coupons/rewards) that have recurring messages that provide a compliant opt-in confirmation message. This message must contain:

- Certified content provider (e.g. “Street Savings”)
- Service description (e.g. “Welcome to Street Savings Alerts”)
- Frequency of messaging (e.g. “Max 3 msg/day”)
- Terms and conditions (e.g. “Msg & Data rates may apply.”)
- Opt-out and customer support information (e.g. “Reply STOP to cancel or HELP for help”)

All short code subscription programs with recurring messages (e.g. coupons/rewards) must contain “Reply STOP to cancel” in each message unless the service utilizes a monthly reminder.

All short code programs must support the universal commands: STOP, QUIT, END, CANCEL, UNSUBSCRIBE, STOP ALL, and HELP.



How to Obtain a Dedicated Short Code

All U.S. short codes are leased through the Common Short Code Administration (CSCA) for three, six, or twelve month terms with renewal options. The cost is \$1,500 per quarter for a random code and \$3,000 per quarter for a “selected” short code.

If a “selected” or specific set of numbers is required for the short code, the first step is to confirm the short code is available with the CSCA at www.usshortcodes.com.

The next step is to submit the text message program’s “campaign details” to the CSCA defining the scope of the program, how the code will be used, the terms and conditions and text message flow.

If the campaign meets the MMA’s established guidelines and best practices, the CSCA will then forward the campaign details as a “program brief” to the individual wireless carriers for their review.

Short codes are provisioned by the wireless carriers and usually take three months. Certification testing is required before any program can be launched to consumers. During the provisioning process, the business will be asked to test its program and submit a certification request. This request will check to see if the program is set up according to the MMA Consumer Best Practice Guidelines and aligned with the campaign details originally submitted to the CSCA. Once the program passes certification, it is now certified and ready for use.

How to Obtain a Shared Short Code

There are many vendors of shared short codes. These vendors should submit campaign details for any business intending to use their short code to the CSCA. The filing fee can vary from \$250 to \$1,000. In addition, these vendors should have a system capable of differentiating program traffic between the shared services.

Shared short codes are aggressively marketed as a way to share the cost of leasing a short code. Since some text message vendors do not submit campaign details to the CSCA for new campaigns on their short codes, wireless carriers continue to tighten requirements for these vendors and are taking action including shutting down shared

³ Common Short Code Administration: <<http://www.usshortcodes.com>>

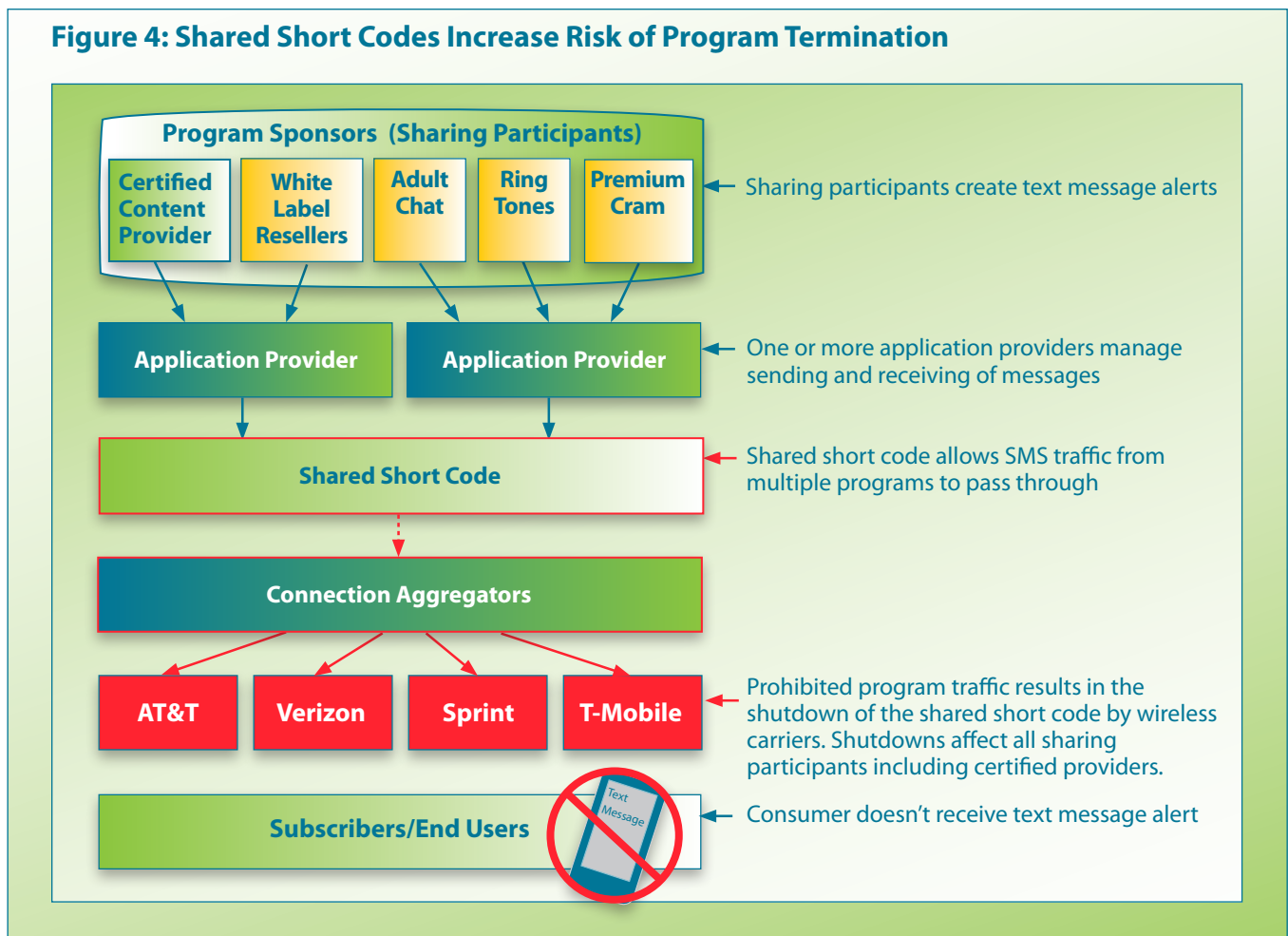
short codes.^{4,5} This is the area of greatest risk for entrepreneurs, independent sales agents, and SMBs who are running mobile marketing programs on a shared short code.

Risks Associated with Shared Short Codes

Despite the difference in operating costs between dedicated and shared short codes, there are significant risks for SMBs using a shared short code. If new campaign details are not submitted to the CSCA on an existing short code (i.e. shared), then the new campaign is in violation. The remedy is to submit new campaign details to the CSCA, pay the appropriate fees and obtain carrier approval. If this is not done, the code (and any associated campaigns) may be terminated.

Even if a business requests that the shared short code vendor submits new campaign details for their program, the business is still at risk because they do not know if the other sharing participants have done the same. It's possible that other sharing participants did not submit campaign details to the CSCA and obtain carrier approval because they are conducting prohibited or "phantom" programs such as adult content, unlicensed entertainment (music etc.) or premium charge cramming (a practice of placing unauthorized charges on a consumer's wireless bill) (Figure 4). There is no way for the business to know if prohibited program traffic is being sent via the shared code. Of course the more sharing participants are involved with a short code, the greater the risk that the wireless carriers will audit and terminate its connectivity.

Figure 4: Shared Short Codes Increase Risk of Program Termination



⁴ Clickatell, "Why am I impacted by the behavior of Clickatell's other U.S. customers?" March 6, 2010, <<http://forums.clickatell.com/index.php?topic=8239.15>>

⁵ Mobile Marketing Watch, "T-Mobile Issues Statement On SMS Lawsuit, Says EZ Texting Didn't Follow The Rules," September 21, 2010, <<http://www.mobilemarketingwatch.com/t-mobile-issues-statement-on-sms-lawsuit-says-ez-texting-didnt-follow-the-rules-9718/>>

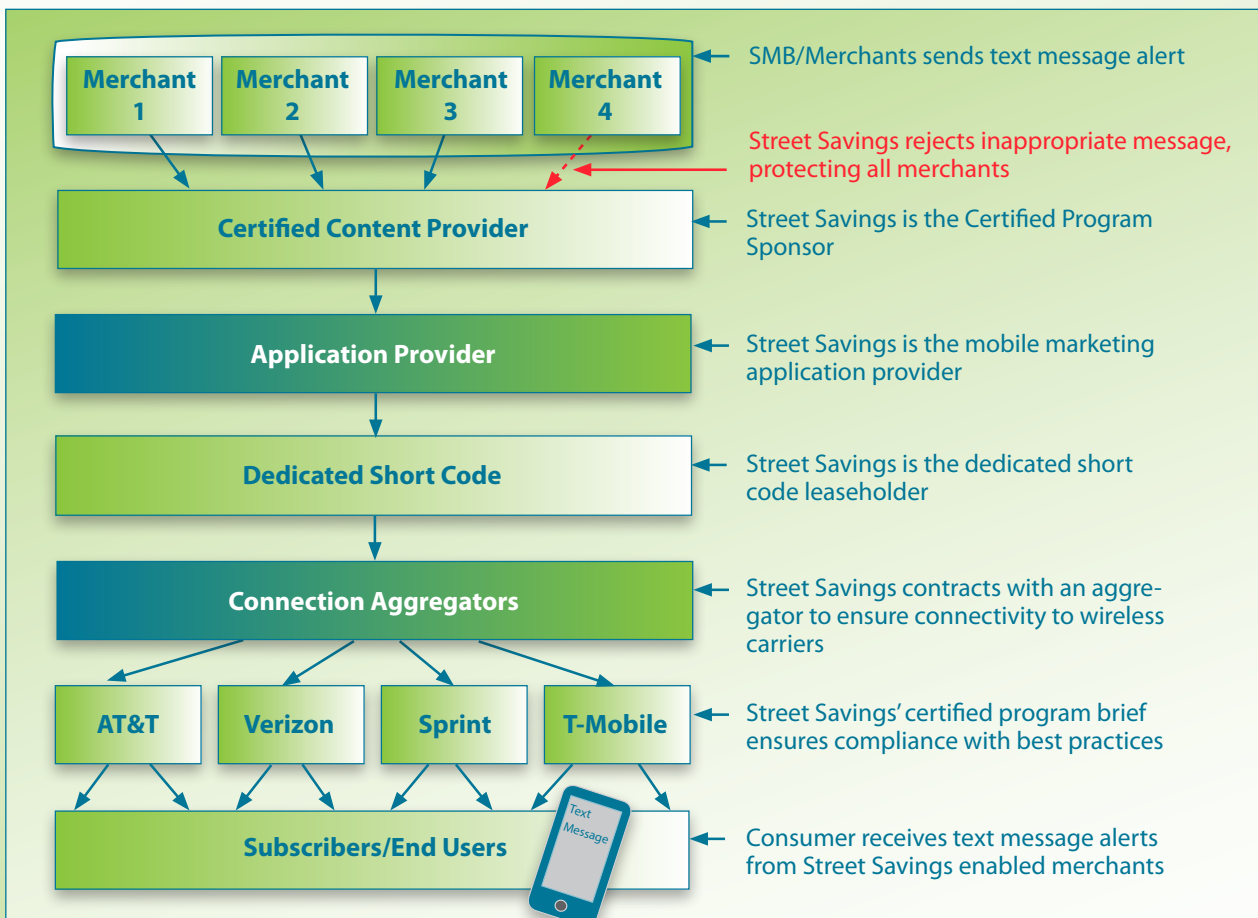
Many shared short code vendors offer “Private / White Label” Reseller packages along with easy to remember short codes. The designation as a “Private” or “White Label” Reseller or the access to a memorable short code does not reduce the risks for the SMB. Unless a “Private/White” Label Reseller uses a dedicated short code with an approved message flow, then the risk to the SMB is the same.

Steps to Avoid Risk

Unfortunately, some shared short code resellers are either unaware of the guidelines or choose to ignore them. It is a “buyer-beware” marketplace. To protect yourself from entering into an untenable business model:

1. Avoid shared short codes altogether.
2. If you are already involved with a shared short code, request that the vendor provide proof that they have submitted campaign details to the CSCA and a filing fee on your behalf.
3. Evaluate your business model to determine if the cost to obtain and provision a dedicated short code and the application to power it, is economically viable.
4. If you cannot justify the expense of a dedicated short code and the application necessary to power it, establish a relationship with a company that does not use a shared short code and has:
 - a. An approved campaign on file with the CSCA
 - b. a certified message flow that supports your marketing,
 - c. an application to power the program.

Figure 5: Street Savings’ Certified, Dedicated Short Code Ensures Compliance



About Street Savings

Street Savings uses a dedicated short code (56687) certified and provisioned in 2006 (Figure 5, p. 6). Street Savings merchants are bound by the Street Savings' campaign on file with the CSCA and its certified message flow including the opt-in/opt-out methods, mandatory disclosure and maximum daily messaging limits shown in Figure 3. Street Savings' certified, dedicated short code ensures that entrepreneurs, independent agents, and SMBs are not at risk with wireless carrier regulations.

Street Savings provides mobile marketing solutions for entrepreneurs, independent sales agents and SMBs that easily and cost effectively mobilize their gift and loyalty programs. The company's Mobile Rewards and Mobile Coupons products utilize mobile text messaging in coordination with existing payment networks, credit card terminals, and Point of Sale (POS) systems to enable merchants to market directly to customers' mobile devices. With Street Savings, businesses of any size and number of locations can quickly and proactively create individualized text marketing campaigns that build brand loyalty and increase sales. For more information, visit www.streetsavings.com

Additional Resources

Mobile Marketing Association, "Common Short Code Primer, version 1.0," June 2006, < <http://www.mmaglobal.com/shortcodeprimer.pdf> >
CTIA - The Wireless Association: <http://www.ctia.org/business_resources/short_code>