CLOUDMARK®

# SMS Spam Overview

Preserving the value of SMS texting

## The value of SMS

Mobile devices have shaped the way we communicate in unprecedented fashion. The small form factor and ease of portability of mobile devices keeps us constantly connected wherever we may be.  This benefit is not being lost on consumers. According to the International Telecommunications Union, there are now over six billion global mobile subscribers for an average global penetration rate of 87%. Counter to logic, phone calls aren't the primary communication taking place on mobile devices – instead it is SMS text messaging. In total, mobile subscribers send in excess of 200,000 SMS text messages every second, according to the ITU.

SMS text messaging offers important benefits over phone or email. The ease and convenience of texting enables its use in nearly every environment without disrupting those around you. SMS texting also leads to near instantaneous response from recipients. Indeed, SMS marketers claim SMS message open rates are higher than 90% and opened within 15 minutes of receipt. Contrast that to the open rate in email of only 20-25% within 24 hours of receipt.

In today's mobile-centric world, companies are also increasingly using SMS to interact with their customers.  Banks are entrusting Mobile Network Operators (MNO) with the delivery of payment authorization confirmations and other financial updates; doctors, dentists and hairdressers use SMS to send appointment confirmations and reminders, and restaurants are adopting it so diners can track wait times. With any interaction, trust is a factor and it appears that most consumers do consider SMS to be a safe and trusted channel of communication.

> *…always-on communications, inherent trust in the channel, high open rates, and six billion subscribers are not lost on those with ill intent.*

Unfortunately, always-on communications, inherent trust in the channel, high open rates, and six billion subscribers are not lost on those with ill intent. Just as SMS provides a successful avenue for legitimate businesses to correspond with its customers, those hoping for illicit profits are also trying to cash in.

## An introduction to SMS spam

Spam is defined as indiscriminate unsolicited messages sent in bulk without opt-in or authorization of the recipient. Spam is ubiquitous and appears in many forms, including email, blog comments, forums, and even poisoned search results.  Increasingly, however, spammers are turning to SMS as a means to reach recipients and elicit illicit revenue. As a result, the number of unique SMS spam campaigns quadrupled in the first half of 2012 and the overall rate of receipt grew by 300% from 2011 to 2012.

### Types of SMS spam

The majority of SMS spam falls into the category of scam or fraud, defined as a campaign to entice the recipient into taking some action that unwittingly results in information disclosure or financial loss. Cloudmark analysis reveals that as much as 92% of SMS spam falls into the scam/fraud category. Social engineering factors heavily in scam and fraud campaigns and, as a result, the exact pitch, or hook, used by the scammer varies by geographical region.

As an example, scams offering free Walmart or Best Buy gift cards abound in the U.S. where the Walmart and Best Buy chains are prevalent and well known. Conversely, SMS recipients in the UK are more likely to receive scams that use PPI compensation or accident claims as the primary hook. Following are examples of the types of concentrated SMS spam abuse experienced in the U.S. and the U.K. in May 2012.

**United States: Top Categories of SMS Spam, May 2012**

Source: Cloudmark

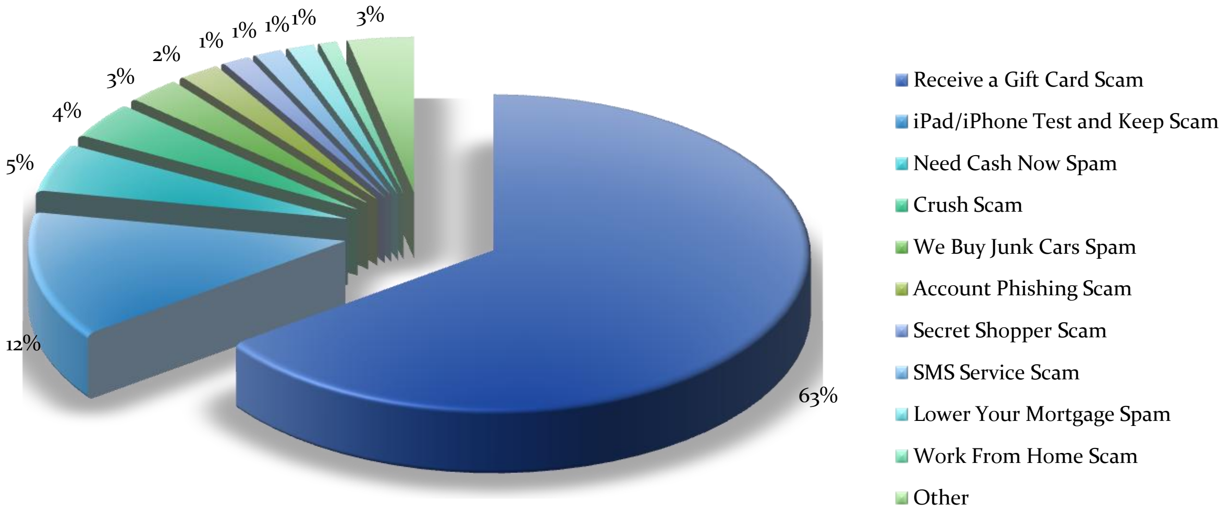
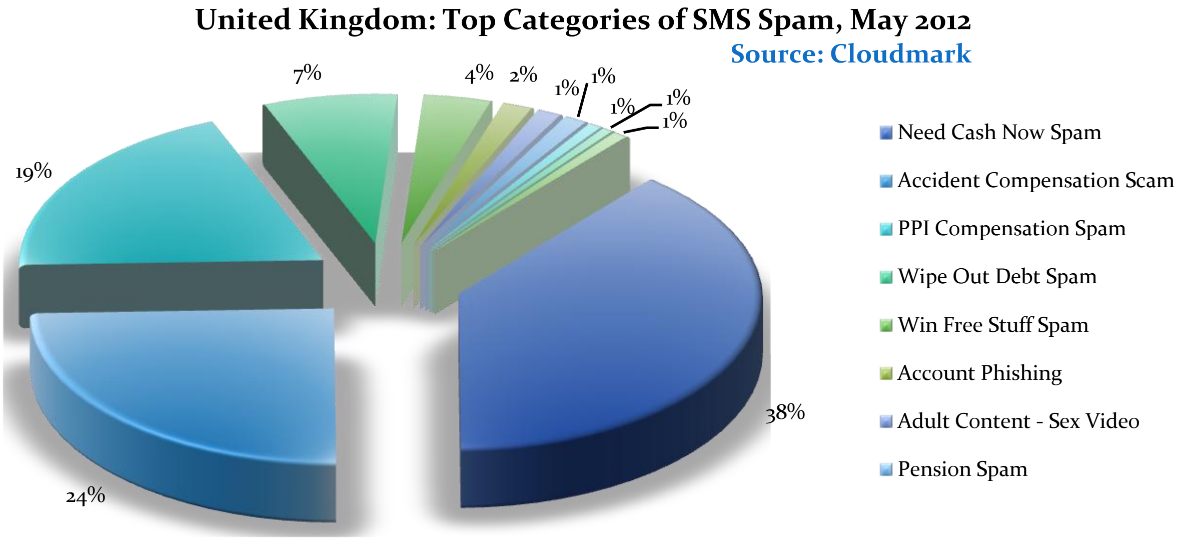


Figure 1


United Kingdom: Top Categories of SMS Spam, May 2012

Source: Cloudmark

Figure 2

### Multi-Faceted Attacks

Scammers seldom work alone. Just as legitimate companies engage in third party partnerships to facilitate their business needs, scammers likewise leverage complex layers of affiliate relations. As a result, the typical SMS text scam is seldom single-purposed; rather each click through or response from the recipient leads to another possible angle to the scam.

For example, a free gift card spam may begin with "just" a survey. However, not only is personal information collected (and sold in aggregate), but the often obscured terms of service for the survey spell out insidious actions such as the inability to cancel the account or an unwitting agreement to send SMS texts to premium rate numbers.

Additionally, the 'free' offer often requires the participant pay a variety of fees in order to continue progressing towards the final 'giveaway' – to the point that even if actual merchandise is ever 'won', the participant has at that point spent more in upfront fees and unanticipated SMS charges than the actual merchandise is worth.

In Australia, the courts recently convicted a fraudster who conned subscribers into making AUS $4m worth of premium rate calls using a fake dating service scam. 1.8million SMS messages were sent, giving a return of AUS $2.40 per message.

## Subscribers' reaction to SMS spam

In many western countries, mobile subscribers view unsolicited messages via SMS as an intrusion of their privacy. Their mobile device often contains their most personal information – contacts, photos and, perhaps most importantly, private text messages. Receiving unsolicited and potentially malicious messages often incenses subscribers, compelling them to call their MNO to complain.

### The effect of SMS spam

Consumers are increasingly opting into mobile services that use SMS as a messaging channel. However, if SMS spam levels in western countries rise to the level experienced in Asia (where as much as 50% of all SMS messages are spam), then subscribers will have difficulty in determining which messages are genuine and may stop responding to any of the SMS they receive.

At best, SMS spam is an occasional irritation to the subscriber. At worst, it can cause a significant financial impact, with bank accounts compromised and premium rate services charged to a subscriber's bill.

The impact on the subscriber depends on the type of attack:

- Unsolicited advertising:
- Inappropriate or adult-themed content
- Premium rate fraud
- Smishing
- Mobile malware

### Subscriber protection

Subscribers can protect themselves from the impact of SMS spam attacks by adhering to the following guidelines:

- Forward SMS spam to short code 7726. If your mobile provider doesn't support 7726, contact them directly o that appropriate counter-measures can be taken. In many cases, MNOs only become aware of an attack when a subscriber reports it (or it has been forwarded to 7726).
- Never click on a link or call a number embedded within an unexpected SMS message, even if it looks like it is from a friend.
- Only download mobile applications from reputable app stores and read the terms of service for each app carefully.
- Never respond to an SMS requesting login details or other personal details, particularly if it claims to be from a bank or other financial institution.
- Don't fall for free giveaways, lottery scams, or other 'too good to be true' offers. Remember, if an offer in an unsolicited SMS seems too good to be true, then it probably is. Companies such as Microsoft, Nokia or your network operator do not run free lotteries for subscribers, nor do reputable banks offer cheap loans via SMS advertising.
- Ask your MNO to set up content filters on your mobile account so that premium rate texts cannot be charged and/or adult material displayed.

## SMS spam and the mobile network operator

Although increased customer knowledge and caution is important in the fight against SMS spam, MNO's also have a vital role to play. How the MNO deals with subscriber complaints of SMS spam and the protection they provide against future attacks will have an impact on customer retention. The negative impact of SMS spam on the MNO includes:

- Increased number of spam-related calls to the call centre ;
- The cost of investigating spam attacks;
- The cost of compensating subscribers for any financial loss experienced;
- Subscriber dissatisfaction and the possibility of churn if subscribers do not believe their MNO is doing enough to protect them from SMS spam;
- The possibility of controls being put in place by regulatory authorities which, for example, can prevent the sale of unlimited SMS or place costly burdens on the MNO.

By safeguarding the network against SMS spam, mobile operators can increase subscriber confidence, reduce bandwidth consumption, and protect legitimate marketing and business use of mobile devices.

MNOs can protect subscribers from SMS spam by implementing a comprehensive, automatically updated messaging security solution which includes:

- A method for subscribers in any region to report mobile abuse quickly and easily, preferably via a common short code or an embedded mobile client  creating a network of global threat intelligence across mobile operators;
- An awareness of SMS message content, protocol and context with carrier-grade accuracy and performance, protecting users before the threat spreads across more users ;
- Support for subscriber-level and operator-level policy controls for security policy decision and enforcement.

To achieve this goal and counter the rise of SMS spam, the GSMA and Cloudmark collaborated to create the GSMA Spam Reporting Service (SRS), a global initiative that enables subscribers to forward SMS spam to their mobile network provider. The MNO automatically forwards the reported message to the GSMA service where it is analyzed using Cloudmark's advanced message fingerprinting technology. The data is then corroborated and an analysis of attacks within the reporting MNO's network is produced.  The MNO can then use this information in their policy management and filtering systems to address the spam in their network.

SRS enables the MNO to:

- Protect Customers: Subscribers react quickly to SMS and may unwittingly fall victim to malicious activity. MNOs can protect their subscribers proactively and immediately by addressing issues at a network level.

- Improve Customer Satisfaction: SMS spam is often seen as a violation of customers' privacy. Empowering subscribers to report spam will lessen frustration and improve the MNO reputation.
- Gain Valuable Network Insight: MNOs can understand the nature and methods of attack on the network and quantify the volume and impact of attacks to develop more efficient security strategies.
- Preserve Brand, Protect Future Revenue: MNOs can attract the highest revenues from the leading global brands with a network that is differentiated by showing security leadership.
- Save on Infrastructure and Support Costs: MNOs can optimize network resources avoiding costly spam, customer support complaints and inter-carrier billing investigations.
- Proactive Regulation: Uncontrolled SMS spam can lead to regulation for subscriber protection. By taking appropriate preventive action and proactively working with regulatory bodies this can be avoided.

Collaboration is also key. To counter the global SMS spam problem, MNOs should collaborate as an industry and share details of attacks, enabling all operators to take the appropriate action. SRS provides detailed reporting capabilities that facilitate knowledge sharing both internally and, if desired, externally with partners.