# Table of Contents

**Highlights** .................................................................................................................. 1  
**Unsolicited Regional Campaigns** ............................................................................... 2  
  Junk Cars Wreck Florida ................................................................................................. 2  
  Top Area Codes for Receiving SMS Spam ...................................................................... 2  
**Mobile Malware** ......................................................................................................... 3  
**General 2013 SMS Spam Trends** ................................................................................ 4  
  Financial Call-to-Actions ............................................................................................... 4  
  Distribution of Financial Call-to-Actions ...................................................................... 4  
  Top SMS Spam Types .................................................................................................... 4  
  iMessage Spam ............................................................................................................ 5  
  Daily Percentage of UK Sports Betting Spam .............................................................. 5  
  Daily Percentage of Auction / Sale Site Spam in the U.S. ................................................ 6  
**Hacked Domains** ......................................................................................................... 7  
  Volume of Spam Using Compromised Domains ............................................................ 7  
  New Compromised Domains By Date .......................................................................... 8  
**Country Report: The United States of America** ......................................................... 9  
**Blocked IP Addresses** ................................................................................................. 10  
  Percentage of IP Address Space Blocked by Cloudmark ........................................... 10  
  IPv6 Traffic .................................................................................................................... 11  
  Blocked IP Address Count By Country ......................................................................... 11  
**Government Involvement** ........................................................................................... 12  
  “Free” Gift Cards Galore ............................................................................................... 12  
  SMS Gift Card Spam, 2012 & 2013 .............................................................................. 13  
**A Look Forward, 2014 Predictions** ............................................................................ 14
During 2013...

- **One in every ten** SMS spam messages landing on U.S. phones ends up in south Florida

- Mobile subscribers in the 954, 305, and 786 area codes reported the **first, fourth, and sixth highest volumes** respectively

- Phishing attempts accounted for **20 percent** of SMS spam reported in the U.S.

- **43 percent** of all SMS spam seen in the UK this past year pushed payday loan offers.

- **Nearly half** of all reported Agentinian SMS spam messages in 2013 offered new cars for sale.

- **67 percent** of SMS spam messages lured U.S. victims with various financial offers.

- Roughly **85 percent** of SMS reports in the UK used money as their pitch.

- A wave of mass iMessages increased auction and retail sales themed spam 36-fold overnight.

- This set of iMessage spam was aimed at the shopping-heavy Thanksgiving holiday and constituted **40% of daily** reported U.S. spam at its peak.

- Cloudmark observed that spammers had compromised well over **two hundred thousand** websites over the past year.

- The U.S. generates about **a third** of the world’s email spam.

- Romania remains in the lead in terms of percentage of IP address space blocked with **22 percent to 25 percent** each month.

- Gift card scams dropped nearly **80 percent** in both volume and monthly percent share shortly after an FTC complaint against 29 defendants was filed.
Unsolicited Regional Campaigns

During 2013, Cloudmark increasingly saw spammers take advantage of location information encoded in phone numbers to send geo-specific spam. While many regions across the globe assign mobile phone numbers to arbitrary, preassigned blocks reserved specifically for mobile devices, many North American and Caribbean countries have taken a different approach. The North American Numbering Plan (NANP) instead assigns numbers, mobile or landline, to the local exchange dedicated to the geographic region in which they are first registered. In these NANP countries, area codes provide a convenient method for correlating phone numbers with a specific geographic region. For instance, New York City’s Manhattan borough is uniquely assigned area codes 212 and 646. While the portability of mobile numbers allows for users to relocate elsewhere and thus introduce an amount of error, these area codes are still largely representative of the population to which they are assigned.

Advertisers, spammers, and attackers in the United States have long since known of this phenomenon and use it to great effect for targeted messaging. For instance, a medical group local to the state of Maryland ran a series of unsolicited SMS adverts this December, 96.4% of which were destined for residents of Maryland and neighboring Washington, D.C. Businesses dealing in physical goods or services, like this one, find they can reach relevant audiences far more efficiently via geo-targeted advertising in comparison to the scattershot SMS campaigns required in other parts of the world.

Junk Cars Wreck Florida

Residents of southern Florida are very familiar with such targeted advertising. The area is home to three of the most popular area codes for SMS spam in the U.S., and it’s not by chance. One in every ten SMS spam messages landing on U.S. phones ends up in south Florida, and more than half of those messages come from a single local company in the business of buying junk cars. Severely limited by the cost and profitability of hauling these junk cars long distances, the spammers choose to focus their SMS adverts on nearby numbers. Cloudmark saw that during 2013, mobile subscribers in the 954, 305, and 786 area codes reported the first, fourth, and sixth highest volumes respectively of SMS spam for any single area code in the US.
Cloudmark also detected a short-term campaign that appeared to use area codes for targeting and tracking effectiveness. In this case, an adult dating site aimed at several metropolitan areas with sizable high tech or oil economies, where they might expect to find a surplus of affluent single males. The campaign targeted each of these area codes with a URL domain specific to that individual area. Doing so enabled the dating site to track the success of this marketing campaign for each area and pitch used in the messages.2

While these area-code specific techniques are not widely used as of yet, they could be problematic should they become widespread. Local attacks may be too low impact to attract the attention of law enforcement and come from businesses too small to be worth suing. However, overall SMS spam levels could see a dramatic rise if unscrupulous businesses all over North America turn to this form of unsolicited, targeted advertising in their local markets.

**Mobile Malware**

A common spam message reported to Cloudmark claims that ‘your bank account is closed.’ Yet, it is simply an attempt to phish bank account credentials. Phishing isn’t the only way for attackers to weasel their way into bank accounts via mobile devices. Many online banking services provide two-factor authentication for login using a mobile Transaction Authentication Number (mTAN) sent by SMS to the user’s mobile phone. Zeus-in-the-Mobile, or Zitmo for short, was one of the first mobile banking trojans to intercept these mTANs back in 2010.3 Since then, many banks have begun providing mobile apps that generate these tokens. Fake token apps have sprung up to capitalize on this by masquerading as the real deal.

One fake token tool, mToken, is able to generate a fake token app with any design required to match a legitimate banking app. It is then able to use HTML injection during a visit to the bank’s website to siphon off information sent between the infected device and the site. SMS messages are also intercepted and sent to a command and control (CnC) server for instances where the victim requests a password reset or receives an mTAN.4

While mToken infections have appeared worldwide, more localized SMS-stealing trojans have popped up this year. The security firm FireEye discovered a Korean malware variant called MisoSMS that used Web-based email to funnel users’ SMS to CnCs in China.5 Korea was also hit by a clever banking trojan masquerading as the Google Play app that would search the victim’s installed apps and overwrite popular banking apps with malicious versions.6 Further west, Kaspersky discovered multiple evolutions of the Android banking trojan Svpeng infecting Russian mobile phones. Disguised as Adobe Flash, the malware used SMS to both collude with its CnCs and direct the victim’s bank to transfer funds into the attacker’s account.7

---

2013 saw SMS spam attacks old and new. Perennially, gift card scams have dwarfed other forms of SMS spam. However, due to an abrupt end to gift card scams last year (more on pg. 14), we observed that bank and account phishing sat firmly atop the list of most prolific SMS spam types in 2013, accounting for 20 percent of the nation’s reported SMS spam. The top category in the UK was a bit more predictable. While the payday lending category saw many lenders abandon the market due to a crack down on shady business practices, 43 percent of all SMS spam seen in the region this past year pushed payday loan offers. In South America, Cloudmark determined that Argentinian cellphones were inundated with a similarly annoying trend offering SMS recipients brand new cars (and the subsequent car loans) simply for showing up with a government-issued ID. Nearly half of all reported Argentinian SMS messages in 2013 enticed would-be car buyers with factory new Fiats and Chevrolets.

**FINANCIAL CALL-TO-ACTIONS**

Money is a powerful motivator, one that spammers around the world exploit to lure victims with the promise of easy cash. These messages using financial motivators vary greatly in severity and content: a fake lottery win demanding a fee to release (nonexistent) funds, compensation for various possible legal wrongs committed against the recipient, fear mongering via the possible loss of one’s own money, and countless other pitches. One constant is the unyielding popularity of money as a hook. During 2013, 67 percent of SMS spam messages lured US victims with various financial offers. Even more staggering is spammers preference for easy money scams in the UK. More than four out of every five spam texts received in the UK, or roughly 85 percent, used money as their pitch.
The UK spammers weren’t entirely focused on money pitches. They are also adopting tried and true marketing techniques traditionally employed by legitimate business. One such example can be attributed to the marketing of online sports betting. Last summer and autumn, as football season kicked off in mid-August, so too did a wave of enticing SMS messages bent on channeling fan fervor. Each Saturday, like clockwork, UK mobiles would see a wave of SMS hit their inboxes while users’ favorite Premier League players hit the pitch. These Saturday sign-up bonus offers were seen spiking above 50 percent of all UK SMS spam seen in a single day. Quickly there after, the category would return to nominal levels until the following Saturday.

**Daily Percentage of UK Sports Betting Spam**

An online retailer using iMessage hit U.S. phones over the week of Thanksgiving, offering sharp deals on designer handbags. Buying habits across the country traditionally ramp up during the holiday winter season, and this vendor was looking to capitalize. Another canny move behind this campaign was the intentional (or perhaps accidental) targeting of iPhone users vs. owners of other mobile devices. IBM reported that over the 2013 holidays season, iOS devices were responsible for five times more online sales than Android devices.¹ With the ease (and scriptability)²-³-⁴ and low cost of sending iMessages, it is no wonder a retailer might augment their holidays advertising from the comfort of their MacBook Air.

**iMessage Spam**

Apple’s over-the-top (OTT) messaging system, iMessage, was a channel for spammers to lower the cost of advertising via SMS last year. While even the cheapest of SMS plans still costs money, iMessage’s design allows users on most Apple devices (iPhones, iPads, MacBooks, and iMacs) to send messages for free over their data plan. The integration of iMessage into the SMS client of iPhones and iPads gives the user an experience that is essentially identical to SMS – for far less money.
Ease and profitability were also likely to blame for the out-of-nowhere surge of this campaign a week prior to Thanksgiving. Overnight, this negligible category for auction and retail sales promotions increased 36-fold to account for more than 40% of all daily SMS spam reported in the U.S. This short period was enough to propel the category’s volume to second highest in November with 18% of reported SMS.

-----------------
2. https://discussions.apple.com/message/19663325#19663325
Hacked Domains

In 2013, we saw a large increase in the use of compromised Web servers by spammers. Spammers use these servers to send spam, provide large ranges of call to action URLs and even host landing pages. A call-to-action URL is the link in the spam email that the spammer wants you to click on. Very often these links do not point to the final destination, but will instead redirect your browser one or more times to the website the spammer wants you to see, which is called the landing page.

There are several reasons for the increase. Though Web servers are less numerous than personal computers, they are generally more powerful, have a high bandwidth connection to the Internet, and are always turned on. They are also often soft targets, running out-of-date and vulnerable software which can be compromised over the Internet, without having to trick a human being into running a trojan or visiting a malicious web site.

We see a variety of techniques being used to compromise Web servers. The most common are exploits in Web publishing platforms, particularly Joomla and WordPress. However, brute force password attacks, malicious code inserted in WordPress plugins and other methods are used. Very often we see more than one spammer using the same compromised domain, either because they have both exploited the same vulnerability, or because access to compromised servers is being sold in the cybercrime underworld in the same way that lists of stolen credit card numbers are.

We have observed that these spammers have compromised well over two hundred thousand websites over the past year. The majority are small business or hobby sites that were set up some time ago and are not being very actively maintained. Very often site...
owners do not have the resources to detect the intrusion, or remediate it if they are notified of it. The result is that in almost half of the cases where a website is hacked, it ends up being taken down, either by the hosting company or victim.

The reaction of hosting companies to this threat has varied. Some have been proactive in detecting and remediating compromised servers, while others have taken little or no action. It seems that, for some, their customers being hacked and their servers being used to facilitate spam are not high priorities. Or, they lack the resources to deal with the problem.

The malware installed by spammers on compromised servers is usually written in PHP and is not as difficult to detect as viruses that infect personal computers. It is quite feasible for hosting providers to scan for compromised servers and begin their remediation process automatically. While some hosting providers provide this service for an additional fee, we feel that it is important enough that it should be included in the basic service, just as spam filtering is provided with any email account.
With a huge number of relatively affluent email users, it’s no surprise that the U.S. is the largest target for spam in the world. What may be more surprising is that the U.S. is by several measures the largest source of spam in the world. In part, this is because as the inventor of the Internet and home to many early adopters, the U.S. has been allocated far more than its fair share of IPv4 addresses. America has 1.5 billion IP addresses. That is more than one third of the entire supply, or about 5 IP addresses for every inhabitant. The country with the next most IP addresses is China, but they only have 0.33 billion, or approximately one IP address for every four inhabitants. Because IP addresses are in large supply in the U.S., they are relatively cheap to acquire, even in large blocks. This makes the U.S. attractive to spammers who are sending from hosting companies. Add to that the fact that the largest webmail companies (which some spammers attempt to exploit) are also located in the U.S., and that makes America the world’s largest source of outbound email spam.

In proportion to the number of Internet users, the U.S. does not generate a huge volume of botnet spam. U.S. users are more likely to update their computers and operating systems frequently than in less affluent and technically sophisticated countries. While a new botnet threat can propagate just as quickly in the U.S. as any other country, it tends to get remediated faster in the U.S. For example, when the Conficker worm first started spreading in 2008 and 2009, it spread as fast in the U.S. as anywhere else, but according to the latest statistics the remaining networks with high numbers of infected machines are in countries such as China, Vietnam, Brazil, Turkey, Taiwan and India.¹

The U.S. generates about a third of the world’s spam. Though three quarters of that is directed at domestic users, the U.S. is also a significant contributor to the spam problem in Brazil, Australia, Japan, Great Britain, Italy, and Switzerland. The U.S. receives spam from almost every country with an Internet connection, though currently there is a disproportionate amount coming from Russia and The Ukraine.

The CAN-SPAM Act of 2003 made the worst forms of spamming illegal in the U.S., but does allow commercial emails, subject to certain restrictions, including an easy way to unsubscribe from future mailings. These rules for large commercial emailers and email service providers make U.S. consumers far better off than those in countries such as Brazil, where there is no anti-spam legislation. However, in spite of several successful prosecutions of spammers, there is still a large volume of spam email directed at U.S. users which disregards the law.

While some of the highest volume spammers hitting the U.S. are based offshore, there are still many that are domestic. Currently over fifty percent of the spammers listed in the Spamhaus. org Register Of Known Spam Operations (ROSKO) are based in the U.S. The CAN-SPAM act removed the right of individuals to bring lawsuits against spammers, and restricted this to ISPs and law enforcement agencies. Yet, neither of these organizations have the resources to bring legal actions against more than a small fraction of the spammers operating from the U.S. Until this changes we do not expect the spam situation in the U.S. to improve.²

2. All spam statistics from the Cloudmark Global Threat Network
Over the course of 2013, we have seen the U.S. overtake Romania and claim first place in the number of IPv4 addresses blacklisted by Cloudmark. The US has far more IP addresses available than any other country, so it has a much smaller percentage of blacklisted IP addresses that Romania - 0.2 percent to Romania’s 22.6 percent. China, the country with the second largest IP address allocation, has also seen a significant upwards trend in the number of blacklisted IP addresses this year, and is now in third place after Romania. Like any other business, spammers attempt to buy their services as cheaply as possible, so the increases in the U.S. and China may simply be due to the fact that IP addresses are cheaper to rent in countries where the supply is greatest.

An increase in the first half of the year put Russia into fourth place, ahead of Germany, which remained reasonably level throughout the year. The blacklisted IP addresses in Germany are due to a very few hosting companies that are providing services to spammers. In fact, three hosting companies account for 50 percent of all the blacklisted IP addresses in Germany. For comparison in the US, the worst seventeen hosting companies account for 50 percent of blacklisted IP addresses.

Romania remains in the lead in terms of percentage of IP address space blocked, remaining consistently in a 22 percent to 25 percent range for all of 2013. There was a brief challenge from Belarus which increased to 28 percent in May, but that country is now down
to 17 percent and falling. Panama has been on an upward trend for most of the year, ending at 12 percent. One Panamanian hosting company is responsible for this. PanamaServer.com accounts for 64 percent of all the blacklisted IP space in Panama. They accept anonymous international clients paying by bitcoin, so they are clearly an attractive service for criminal enterprises.

When the U.S. government relaxed sanctions on the sale of laptops and other computer equipment to Iran in May 2013, we saw an increase in the percentage of blacklisted Iranian IP addresses from 1.8 percent in June to 3.9 percent by the end of September. However this seems to have stabilized and is now down to 3.2 percent.

**IPv6 Traffic**

IPv6, which has a vastly larger address space than IPv4, has been adopted by some ISPs for inbound email. In 2013 we saw some very high volume spam attacks transmitted via IPv6 where this was supported. Traditional blacklisting of individual IP addresses is not effective for IPv6 as there are too many addresses available. Sender reputation under IPv6 must be based on domains and/or address ranges, often at the /32 and sometimes as broad as a /29 or /22 level. Unknown senders are held in a lower class of service and rate limited until it is established that they are reputable. We have found this to be effective in dealing with IPv6 attacks, and we are working closely with our clients and industry representatives to refine this approach as IPv6 becomes more prevalent for sending and receiving email.

![Blocked IP Address Count By Country](chart.png)
While instances of SMS and email abuse are continually evolving, legal intervention is becoming ever more common this year in jurisdictions around the globe. In Chile, the consumer protection service known as SERNAC leveled charges in early 2013 against three mobile operators in the country for their SMS spam abuse. Claro, Movistar, and Entel faced fines of a combined $86 million due to SMS advertising campaigns that lacked evident means to opt-out, discern cost, or properly judge the offers’ terms. The Telecom Regulatory Authority of India (TRAI) has taken an even harder line against unwanted marketing calls and texts. Previously, TRAI implemented fines for sending these unsolicited messages, but the problem persisted. Under current regulations, telemarketers in several key markets, such as banking, insurance and realty, which are caught originating unsolicited texts or calls face outright bans from bulk communication mediums. TRAI has also put into effect a fine against transgressing mobile operators who are complicit in ferrying the unsolicited commercial calls or texts. The fine imposed is Rs. 5,000 per verifiable complaint - a potentially costly mistake in the realm of bulk messaging. In the UK, police made several arrests of spammers sending text messages offering to provide cash payments from pension funds before they mature, and the Information Commissioner’s Office fined one company £175,000 for sending text messages promoting payday loans.

The United States rolled out a similar fine in the later part of the year. The Federal Communications Commission expanded the current Telephone Consumer Protection Act (TCPA) to penalize anyone responsible for sending marketing SMS without first receiving written consent from the intended recipient. Those who don’t heed the TCPA’s guidelines open themselves to potential consumer damages up to $1500 USD per text message. The TCPA has already enabled consumers to seek damages. One instance of which involved Jiffy Lube settling a class action suit for roughly $47 million. Requiring prior written consent tightens the act’s mandates.

“Free” Gift Cards Galore

One crackdown stood out from all others as the most visibly effective legal action taken against spammers in 2013. On March 7th, the Federal Trade Commission (FTC), a U.S. regulatory agency that oversees business practices and consumer protection, announced that it had filed a series of complaints against those allegedly responsible for sending hundreds of millions of “free” gift card SMS messages. Many U.S. mobile subscribers are likely to be well acquainted with these spam texts. Messages would arrive offering an enticing, “free” gift card from one of several major retailers. Best Buy, Target, and Walmart’s names were all used in the ruse. However, if a recipient tried to take up the offer by following the link provided, no real gift card came. Instead the user was directed to a site asking for various personal details to qualify and receive the gift. Unfortunately, many victims don’t know that it sat behind an impossible Terms of Service Agreement that prevented victims from ever receiving the card. Instead of a receiving a gift card, victims’ efforts to qualify via registering for various extraneous services was just a means for the perpetrator to monetize through a list of affiliate marketing programs. This string of affiliate actions would net the perpetrator significant referral income at each stage. Victims’ personal information was also often sold in bulk for various other uses.
As can be seen above, more than half of all U.S. spam texts during each month were gift card spam during five months of 2012. The sheer volume of the gift card SMS resulted in it remaining the most common type of spam during eleven months in 2012. In total, this singular form of spam accounted for 44 percent of all U.S. SMS spam reported throughout that year. The category continued to flood U.S. mobile phones unabated at the start of 2013.

Things drastically changed when the FTC filed complaints against 29 defendants. The Commission claimed that these parties were responsible for sending more than 180 million spam texts, imposing a financial burden on recipients who were forced to pay for delivery charges. Seemingly over night, the levels of gift card spam plummeted. Cloudmark detected that volumes subsided so harshly in the wake of these filings that gift card spam was just 6 percent of March’s SMS spam. This nearly 80 percent drop in both volume and monthly percent share was not a short-term effect. The category as a whole has almost entirely dried up. During the second half of 2013, levels of gift card spam remained steadily below two percent.

1. http://blog.cloudmark.com/2013/05/10/3-mnos-in-court-for-sms-spam/
A Look Forward, 2014 Predictions

Government interventions and regulations will likely continue in the coming year. Throughout 2014, regulators in nascent mobile markets will likely roll out stringent penalties against transgressing spammers. Mature markets may struggle with established, shortsighted regulations but will battle to tighten laws. Mobile operators are also inclined to revive their focus on providing “clean-pipes” via SMS. As subscribers look to carriers for protection from increasing abuse, premium rate texts will become a crucial focal point in the debate. If not, users may dump SMS for cheaper solutions in the form of over-the-top (OTT) messaging.

Without intervention, inherently malicious messages and mobile malware will continue to plague mobile networks even more during 2014. The unabated incidences of phishing-related mobile trojans and SMS phishing attacks suggest that attackers had noticeable success with these techniques, and they show no signs of slowing. SMS won’t be alone. In the later months of 2013, CryptoLocker ransomware reaffirmed that malicious emails are far from a dying trend. Together, each of these suggests that perpetrators will look to more directly influence their Return-On-Investment (ROI) using surreptitious means this year.

Spammers will also look increasingly to monetize SMS advertising in 2014. In the first half of 2013 alone, the IAB estimated that Internet advertising revenues had reached $20.1 billion. SMS will be an attractive vector for cashing in on these bulging referral programs. Despite crackdowns, fraudulent campaigns will continue to be designed around PPI compensation, pension liberation, and similar programs which benefit from wide publicity and the tendency for financial strapped victims to fall prey to such enticements. In the U.S., healthcare reform, commonly known as “Obamacare,” is likely to fall prey to similar tactics in 2014.

OTT networks may experience the unwanted attention of spammers. With mounting legislation and risk associated with SMS, spammers will begin using OTT even more. We’ve already seen this recently in form of iMessage spam hitting iPhone users. These OTT providers benefit greatly from a very closed ecosystem that they can tightly control to better stem the tide of new spam. Those that don’t clamp will quickly lose users to increasing competition.

Social networks, while burdened with the potential for spam, will be concerned with ensuring privacy. Personalization and targeting are highly valuable to scammers and spammers looking to increase their ROI. Scraping social profiles for personal information, posts, and habits provides an easy shortcut to all kinds of abuse, including: phishing attacks; IRS tax return fraud; and reselling personal details to insurance companies, credit agencies, etc. for direct sales and marketing.

A prime example of these privacy concerns came in the final days of December. The API of popular social app, Snapchat, was hit with a disclosure that has opened the door for a new wave of targeted spam and scams to hit phones in 2014. The disclosure by security group Gibson Security highlighted an easy method for scraping large sums of username and phone number pairings of registered users via the app’s readily accessible API. The attention surrounding this event will undoubtedly attract less scrupulous individuals to weaknesses in Snapchat’s API.

Early in 2013, Facebook was privy to similar scrapping. The fruits of this labor quickly made
their way into SMS spam as the correlated data sets were used to send individuals SMS spam custom-tailored with their first name. Facebook was extremely proactive in dealing with this. It’s possible that the same may happen in 2014 with Snapchat usernames tied to the scrapped phone numbers unless Snapchat is as aggressive as Facebook was in dealing with this sort of data mining.

About Cloudmark

Cloudmark builds messaging security software that protects communications service provider networks and their subscribers against the widest range of messaging threats. Only Cloudmark Security Platform™ delivers instant security and control across diverse messaging environments, enabling communications service providers to create a safe user experience, protect revenue and safeguard their brand, while streamlining infrastructure and reducing operational costs. Cloudmark’s patented solutions protect more than 120 tier-one customers worldwide, including AT&T, Verizon, Swisscom, Comcast, Cox and NTT.