# Cloudmark 1Q13

## Global eMessaging Threat Report

**January – March 2013**

# Crackdown on SMS Gift Card Scams

### The Federal Trade Commission, an American regulatory agency, charges 29 defendants with sending 180 million gift card themed SMS spam messages.

On March 7th, the Federal Trade Commission (FTC) announced that it was filing a series of complaints regarding abusive use of SMS messaging services to send more than 180 million scam messages. These scam messages falsely promised individuals "free" gift cards or prizes from retailers such as Best Buy, Walmart, and Target. Unfortunately, victims are tricked into providing personal information and signing impossible terms and conditions that void any possibility of winning. In the unlikely event a prize is won, the recipient ends up paying more to receive the prize than the product's value. These types of scams have dominated the reports to 7726 by a wide margin. Gift card scams constituted 44% of all SMS spam reported in 2012. The eight complaints filed by the FTC seemed to have also had a noticeable affect on the volume of gift card scams sent out in the first quarter of 2013. Figure 1 clearly demonstrates the impact that this move had on spam volumes. Daily rates fell dramatically from near 50% to below 10% of volume during the days leading up to and after the announcement.

**Figure 1. Daily Volume of Recieve a Gift Card Scams in the U.S., 1Q13**
**Source: Cloudmark / GSMA**

# Job Listing Scams and Adult Content Spam show big gains throughout 1Q13 with even larger gains in the wake of a U.S. gift card scam crackdown.

Two relative newcomers joined the quarterly top 5: Job Listing Scams and Adult Content Spam. Both are by no means new to the world of email or SMS spam. However, their recent surges in SMS volumes have landed them in the spotlight this quarter. Although both types of spam rarely contributed more than 5% of monthly volumes in 2012, both have more than doubled already this year. As expected, Receive a Gift Card Scam claimed the number one position due entirely to its dominance in January and February. The FTC's charges came late in the quarter.

**Figure 2. Top 10 Attack Types, 1Q13**
Source: Cloudmark / GSMA

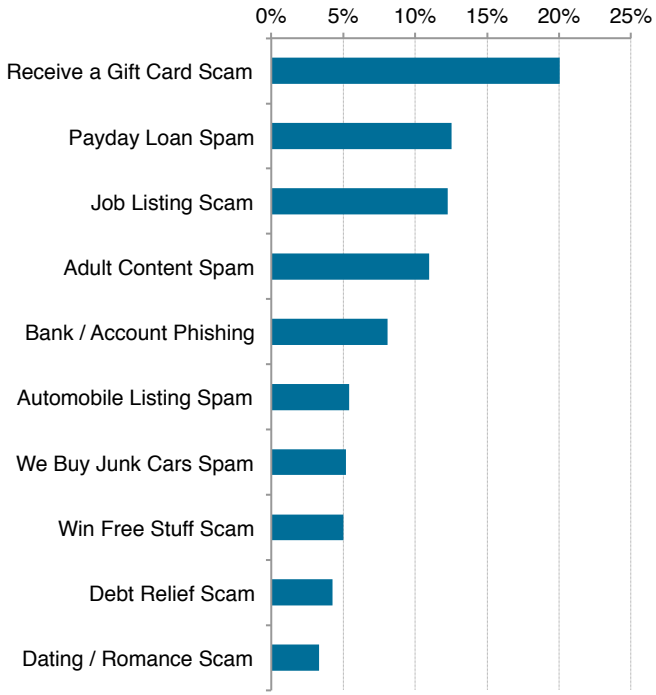
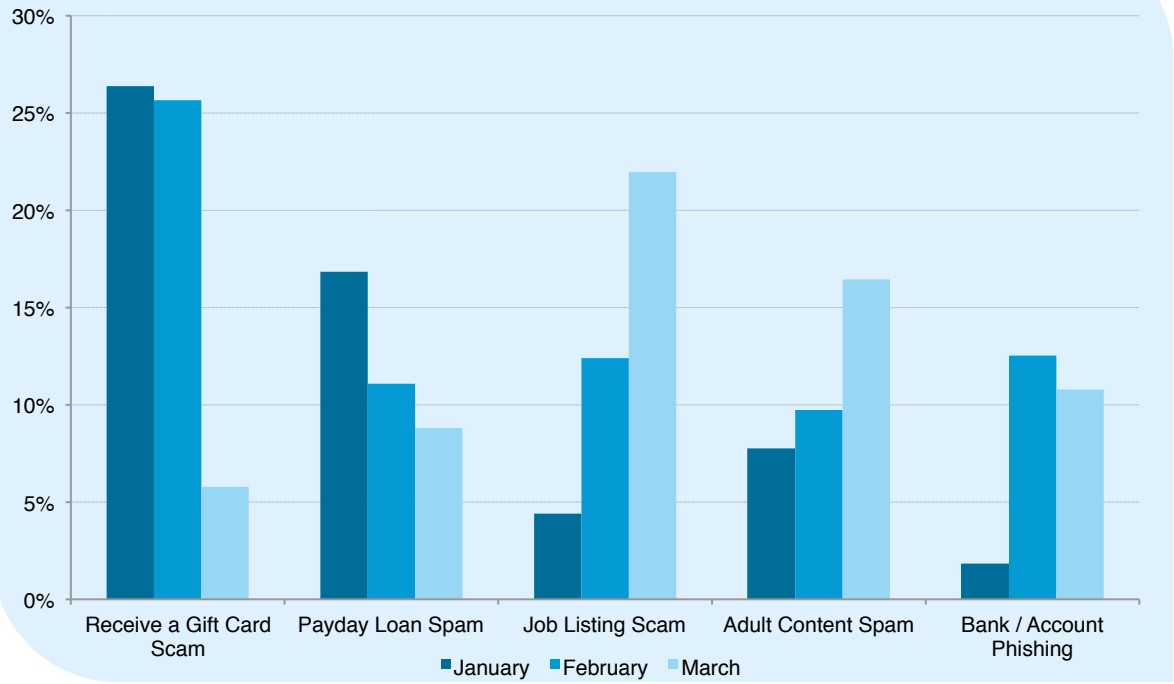



Figure 3 illustrates the monthly volumes of the top 5 categories over 2013's first quarter. Job Listing Scam volumes exploded by 400% over the quarter by increasing its 4% share up to 22%. Meanwhile, gift card volumes plummeted by 78% with a measly 6% share of March's volume, barely enough to make March's top 5. Phishing attacks also seemed to be on the rise in February and March with double-digit shares.

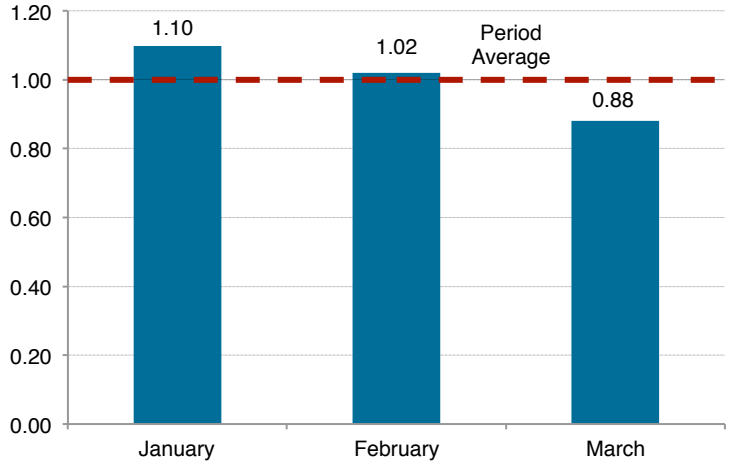
**Figure 3. Monthly Volumes of the Quarter's Top 5 Attack Types, 1Q13**
Source: Cloudmark / GSMA



# Gift card scam crackdown roughly correlates to dramatic declines in average monthly volumes. Uptick in Bank and Account Phishing may be linked to approaching U.S. tax season.

Figure 4, below, represents the total number of reports to 7726 normalized by the quarter's average volume. This figure shows a near 20% drop in the volume of reports from January to March. The likely culprit: gift card scam volumes plunging.

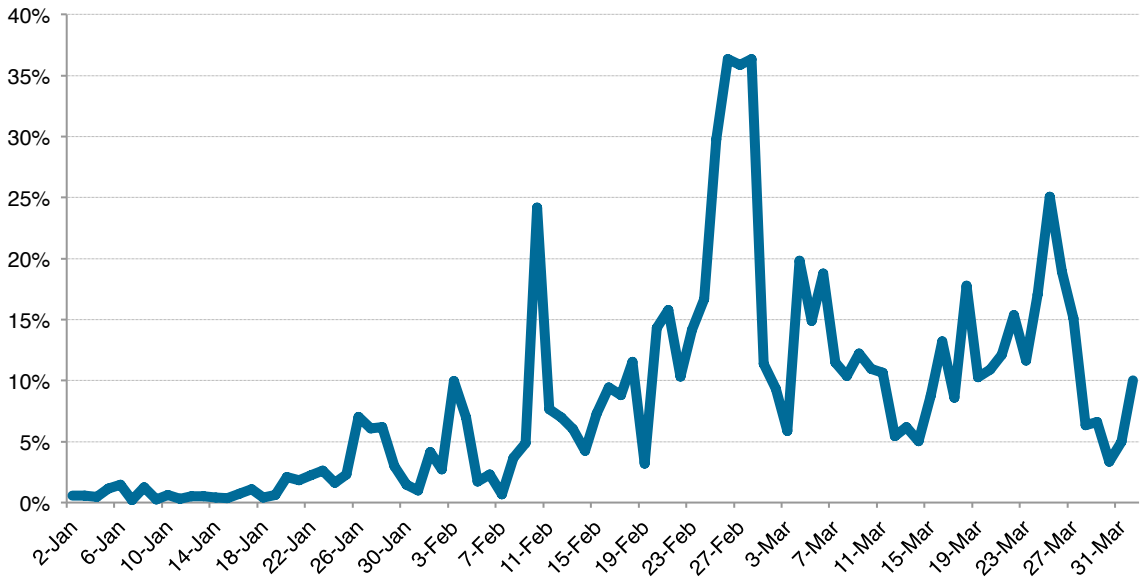
**Figure 4. Monthly Reports Normalized by Average**
**Source: Cloudmark / GSMA**




It would be expected to consistently see increases in reported volumes. Other variables may have played a part in this decline. A slight decrease was seen in February, but Gift card scams only saw noticeable decline in March. It is plausible that Payday Loan Spam's noticeable drop in volume drove February's dip. Spammers may also be consolidating their efforts into more potent messages to help elevate their return on investment.

SMS phishing attempts are one plausible way for attackers to do this. With phishing, victims run the risk of losing sensitive personal information, bank accounts, and credit/debit cards. Even just a single victim can provide an extremely lucrative return on investment. Attackers are likely looking to capitalize on this in conjunction with the U.S. tax season to swindle victims of the money saved up for the April 15th deadline along with future tax returns. Figure 5 illustrates the prominent peaks in SMS phishing volumes throughout the quarter. A very similar trend was seen in September and October leading up to the United States' tax filing extension deadline, October 15th.

**Figure 5. Daily Volume of SMS Bank / Account Phishing**
**Source: Cloudmark / GSMA**



Cloudmark Global eMessaging Threat Report

Highlighting spam and scam trends observed in SMS and email from January 1, 2013 – March 31, 2013

# Country Profile: Panama

## Several Panamanian services may help spammers and botnet herders remain anonymous, but genuine criminal activity is not condoned.

In the past year Cloudmark has detected several high profile attacks with links to Panama, including the SpamSoldier Android botnet and the Grum PC botnet. These are the result of two companies that do not attempt to prevent spammers using their services. They are Internet.bs and Panamaserver.com.

Internet.bs is a domain registrar that, according to LegitScript, provides registration services for one third of all rogue online pharmacies. It is also responsible for several of the domains used by the SpamSoldier Android botnet attack. Though .bs is technically a Bahamian domain, both the Chairman (Gregg McNair) and the CEO (Marco Rinaudo) of Internet.bs are Panamanian residents.

The privacy service provided with Internet.bs registration is Fundacion Private Whois, a Panamanian corporation. Yet, their web site, privatewhois.net, is hosted in London by safeukdns.net, which in turn is registered by contactprivacy.com in Canada.

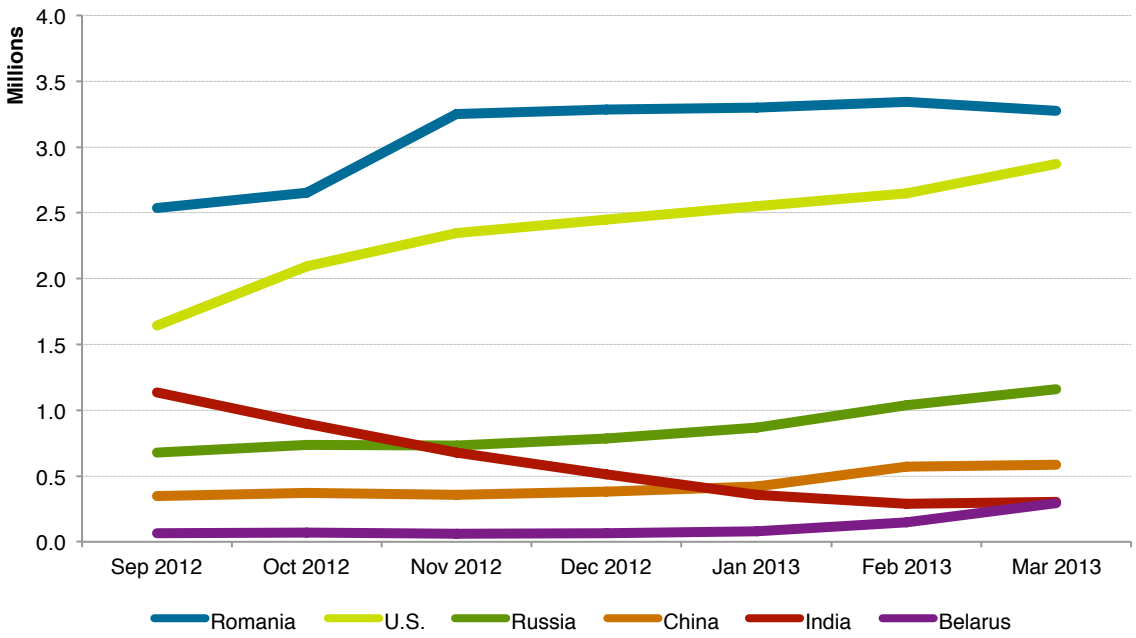
Panamaserver.com is a hosting service that accepts anonymous customers paying using Web Money or Liberty Reserve. Along with a Panamanian phone number, they have contact numbers in the US and Brazil, and their web site stresses the “offshore” nature of their operations. Most of the spam seen from their IP addresses is unsolicited bulk marketing email to customers in Brazil. Since neither Panama nor Brazil has any anti-spam laws, this is perfectly legal. Cloudmark currently has more than 80% of their IP address space flagged as poor or suspect as a result of this spam activity.

Panamaserver's hosting is not completely bullet proof. Two of the Command and Control servers for the Grum botnet were traced back to their IP address space last year. Unfortunately, these servers were only taken down in response to international pressure.

# Blocked IP Addresses By Country

The following chart shows countries that have demonstrated a significant change in the volume of IP addresses recommended for blocking by Cloudmark.

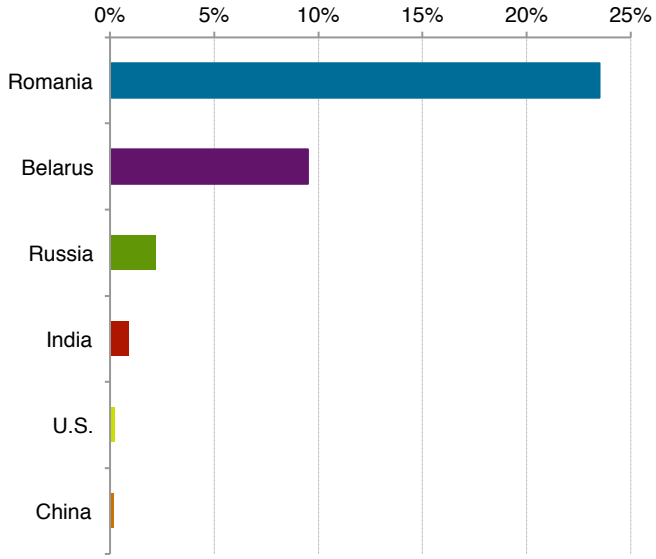
**Figure 6. Blocked IP Address Count By Country**
Source: Cloudmark




Romania appears to have hit a plateau with marginal decline last month. However, we are seeing a corresponding increase in the figures for Belarus. It seems likely that some of the spammers using Romanian hosting services are starting to transfer their activities to Belarus. The US is in second place for absolute number of IP addresses blocked. This represents a far smaller percentage of the total address space for the country than Romania though. India is showing consistent improvement after several reports last year that it was a major source of spam in the world. China and Russia are both showing consistent, long-term increases.

To the right is each country's percentage of address space currently blocked. As noted previously, the total number of IP addresses blocked in the US and Romania (Figure 6) are comparable. Yet, such volumes represent only 0.2% of the US address space. Meanwhile, 23.3% of Romanian IP addresses are blocked. Similarly, Cloudmark is currently blocking about twice as many IP addresses in Russia as in China, but this volume is 2.5% of Russia's total address space. China's blocked addresses only account for 0.2% of the country's address space.

**Figure 7. Percentage of IP Address Space Blocked by Cloudmark**
Source: Cloudmark



# About Cloudmark

**Cloudmark** builds messaging security software that protects communications service provider networks and their subscribers against the widest range of messaging threats. Only the 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.

*The Cloudmark Global Threat Network protects over 2 billion subscribers for the world's largest networks.*


## Cloudmark Headquarters

128 King Street
Second Floor
San Francisco, CA 94107

Telephone: +1-415-946-3800
Fax: +1-415-543-1233
Email: sales@cloudmark.com

## Cloudmark Europe, Ltd

Davidson House
Forbury Square
Reading, RG1 3EU
United Kingdom

Email: emea@cloudmark.com

## Cloudmark Labs

41 Boulevard des Capucines
75002 Paris France

Telephone: +33 (1) 80 48 08 20
Fax: +33 (1) 45 26 18 10
Email: paris@cloudmark.com

## Cloudmark Singapore

3 Temasek Avenue
Centennial Tower, #21-07
Singapore 039190

Telephone: +65 6549 7845
Email: apac@cloudmark.com

## Cloudmark Japan

Hibiya Central Bldg. 14F
1-2-9 Nishi-Shinbashi, Minato-ku
Tokyo 105-0003 Japan

Telephone: +81 (0)3 5532 7636
Fax: +81 (0)3 5532 7373
Email: japan@cloudmark.com