CLOUDMARK
Mobile Security Solutions Guide
Executive Summary ........................................................................................................................................... 2

How Can Cloudmark Help You?...................................................................................................................... 3
Your Network is Burdened with Unwanted SMS Spam, Generating Support Calls and Increasing Your Operating Costs ......................................................................................................................... 3
Mobile Subscribers Are Requesting Personal Security Features ........................................................................ 3
Reducing Churn and Customer Dissatisfaction .................................................................................................. 3
You Would Like to Control Revenue Generating Opt-in Advertising by Third-Parties .............................................. 4
Revenue Leakage is Reducing Your SMS Messaging Profits ................................................................................. 4
Fraudsters Are Using ‘SIM Boxes/Farms’ to Spam Your Subscribers ................................................................. 4
Your Outbound Traffic is Costing You Because it is Full of Spam ....................................................................... 5
Applications and Infected Devices Are Generating Large Amounts of Spam on Your Network ........................................ 5

Mobile Operator Challenges ............................................................................................................................... 6
Mobile Phones are Personal ................................................................................................................................. 7
Mobile Apps and Trojan Malware ....................................................................................................................... 7
Messaging Fraud is Eroding Subscriber Trust and Operator Profits ...................................................................... 8

The Cloudmark Mobile Security Solution .......................................................................................................... 8
Cloudmark Mobile Platform ................................................................................................................................. 9
Sender Reputation ................................................................................................................................................ 9
Traffic Intelligence ............................................................................................................................................... 9
Message Fingerprinting ...................................................................................................................................... 10
Message Control by Protocol .............................................................................................................................. 11
Message Control by Content ............................................................................................................................... 11
MMS Message Control ......................................................................................................................................... 11
Workflow-based Framework .................................................................................................................................. 11
Web-based Management ....................................................................................................................................... 11
Customizable Logging and Reporting ................................................................................................................. 11
Value-added Services .......................................................................................................................................... 12
Seamless Network Integration ............................................................................................................................ 12
Carrier-class Scalability, Reliability and Performance ............................................................................................ 13
Cloudmark Sender Intelligence .............................................................................................................................. 13
Cloudmark Authority .......................................................................................................................................... 13
The Cloudmark Global Threat Network ............................................................................................................... 14
GSMA Spam Reporting Service (SRS) .................................................................................................................. 14

Summary ............................................................................................................................................................... 15
Executive Summary

Over the past 25 years, mobile operators have done a superb job in providing secure and trusted voice communications, messaging, internet access and a wealth of other valuable services. Careful planning and execution have rewarded operators with exponential increases in mobile users, service revenues, and profits. In 2015, mobile operators brought in more than US$1 trillion in revenue. However, since the start of this decade, changes in the mobile landscape are threatening to undo years of hard work, putting SMS, MMS and other services at risk, while negatively affecting subscriber trust and operator profits.

Major trends driving these changes include the exposure of mobile operator networks to external services such as the internet, the proliferation of smartphones, decreasing messaging revenues, and the growing popularity of ‘over the top’ or OTT services such as Apple iMessage, Google apps, Facebook Messenger, WhatsApp, and Snapchat. As subscribers rely on mobile phones for all communications, including financial transactions, they have become attractive and lucrative targets for attackers. A subscriber’s trust is directly impacted when they receive malicious messages and malware through a supposedly trusted service. Abusive traffic also increases costs for operators by wasting valuable network resources, increasing customer care costs and customer churn, and threatening subscriber adoption of future mobile services from the mobile operator.

As operators develop more value-added services to enhance their revenue streams, they must work even harder to preserve the trusted user experience that subscribers have come to expect. It is critical at this time of technological advancement and increased threat risk that operators work to secure their networks and revenue with a comprehensive messaging security solution. Cloudmark, the undisputed leader in mobile messaging security, has earned the trust of more than 120 operators and 2 billion subscribers worldwide. With demonstrated expertise in developing the fastest and most scalable messaging security solutions, Cloudmark protects the world’s largest mobile operators against the latest mobile spam, phishing, grey routes, and malware attacks. Cloudmark offers mobile operators the following benefits:

- **360-Degree Messaging Security** – Scans all inbound and outbound SMS, MMS, RCS, social networking, web browsing, email, and other messaging traffic to protect operator networks and subscribers against all types of mobile spam, phishing attacks, and malware. Blocking outbound spam protects your company’s reputation with receiving ISPs, reducing throttling and IP address blacklisting, as well as ensuring that any balance of message traffic is not impacted by outbound spam.

- **Fast Threat Response with Unmatched Accuracy** – Cloudmark detects and blocks mobile spam and threats using information from the Cloudmark Global Threat Network (GTN) and advanced algorithms refined over 14 years. The GTN feeds up-to-the-minute spam and threat intelligence from more than two billion user accounts worldwide to Cloudmark security solutions.

- **Flow control and traffic analysis** – Cloudmark monitors the traffic in the network to allow identification of different traffic patterns and types of users in the system. By allocating senders to specific classes of service and using this reputation, the system can not only monitor traffic but also
proactively report and restrict senders when changes in patterns occur, allowing for the highest level of network protection.

- **Cost and Overhead Reduction** – Cloudmark scans all messages with minimal processing requirements, drastically reducing necessary hardware and freeing system resources. Security automation and simplified management frees system administrators for other tasks.

- **Low Latency Message Scanning** – Less than 10ms scanning latency reduces network impact and maintains subscriber service levels.

- **High Reliability and Scalability** – Cloudmark's carrier-class solutions enable operators to provide secure messaging services to business customers with the highest levels of reliability, scalability and availability.

**How Can Cloudmark Help You?**

The Cloudmark Mobile Security Solution solves a wide variety of problems facing operators today. Below are some of the ways Cloudmark can help your organization.

**Your Network is Burdened with Unwanted SMS Spam, Generating Support Calls and Increasing Your Operating Costs**

Attackers seeking access to your mobile subscribers can clog your network with unwanted spam and fraudulent messages. Cloudmark Mobile Security Solutions scans all inbound and outbound SMS, MMS, RCS, social networking, web browsing, email and other messaging traffic to protect against all types of mobile spam, phishing attacks, and malware. Cloudmark stops abusive traffic before it enters your network; freeing up bandwidth, improving stability and reducing operational costs and overhead. It also scans messages in transit to ensure that in-network devices and partners are not creating abusive traffic inside your network. Your subscribers will enjoy a secure experience, improving brand loyalty and acceptance of value-added services.

**Mobile Subscribers Are Requesting Personal Security Features**

Cloudmark enables you to offer a variety of value-added per-subscriber services to your customers such as sender block and allow lists. In addition, the Cloudmark Mobile Platform can integrate with whitelist and blacklist data sources, enabling paid subscriber services such as anti-bullying, and parental control.

**Reducing Churn and Customer Dissatisfaction**

Mobile messages are a disruptive event for the mobile subscribers and thus tend to get very high read rates. Mobile subscribers impacted by poor protection from abuse blame their provider for the spam and lack of security features. These subscribers' tolerance for continued abuse is very low and
unless security is provided, users either stop using the carrier functionality and move to OTT solutions or change provider to one that have better protection.

**You Would Like to Control Revenue Generating Opt-in Advertising by Third-Parties**

Cloudmark enables revenue sharing with third-party marketing and advertising companies by enforcing messaging categories based on subscriber preferences. For example, limits can be applied to message volume on a daily or weekly basis, polices can filter messages according to content or source, and smartphone applications can be downloaded for reporting abuse. Third-party marketing databases can be seamlessly integrated for access to subscriber preference data.

**Revenue Leakage is Reducing Your SMS Messaging Profits**

Sometimes legitimate traffic requested by users is delivered via illegitimate means. Inappropriate bulk sending agreements, or the use of foreign operators without interconnect contracts can allow third-party messaging entities to avoid proper payment for message delivery. For example, an airline using a foreign external short messaging entity (ESME) to send flight information to their customers. Subscribers will receive the messages but the home operator may not receive a mobile termination fee, or be able to control the amount of messages sent by the aggregator as they are sending commercial messages in exactly the same way as person-to-person messages.

Cloudmark incorporates advanced on-net/off-net threat detection technologies to stop 'grey market' revenue leakage and restore messaging profits. Most anti-spoofing, flooding, and faking solutions use protocol level controls to counteract signaling fraud between mobile networks, but Cloudmark goes beyond to catch mobile attacks that may have already entered your network.

**Fraudsters Are Using ‘SIM Boxes/Farms’ to Spam Your Subscribers**

In an effort to combat spam, operators impose limits on the number of SMS messages that a given SIM card or MISDN can send on their network. In order to get around this defense, fraudsters load multiple SIM cards into a chassis-based system and send a limited number of messages from each card. They also use software solutions and third-party aggregators or integrators to perform the same type of service. The attackers simply modify the sending numbers and/or the message contents and continue the attack ignoring any imposed rate limiting/blocking. Cloudmark includes powerful analytical tools which can be used to identify SIM boxes and other systems, allowing the expansion of sending campaigns over many sending numbers and even different networks.
Your Outbound Traffic is Costing You Because it is Full of Spam

The proliferation of outbound spam can cause an unprotected operator’s reputation to fall and for other carriers to block its sent messages. This may mean mobile legitimate subscriber messages failing to be delivered. This generates end user dissatisfaction and even increases churn as users move to providers (either different carriers or applications) that can deliver their messages reliably.

Applications and Infected Devices Are Generating Large Amounts of Spam on Your Network

Specific applications offer free messaging or even money to the end user for allowing the application to quietly use the device as a sending system inside the mobile operator’s network. This works like a botnet without the user realizing (or caring) that they are now a source of spam in the network. Detection and isolation of such compromised devices is becoming an issue for operators. These devices can be the source of spam inside the network and are very hard to detect by other means as their traffic is mixed with normal user traffic. Cloudmark detects, tracks, and reports on such infected/malicious devices through behavioral analysis. Offenders can be redirected to walled gardens, and dealt with specifically while not affecting the other devices in your existing network.
**Mobile Operator Challenges**

Billions of consumers and corporate subscribers have come to rely on their mobile phones for a myriad of both critical and routine tasks including the secure exchange of critical business information, driving directions, and personal banking transactions. Network connectivity offers subscribers real-time access to the vast resources of the Internet, whilst smartphone platforms, applications and services bring desktop processing power and flexibility to mobile devices. Smartphone and tablet users can now easily manage personal and corporate email, edit photos, manipulate documents, and even participate in video conferences.

As mobile and fixed networks converge, along with social networking applications they support, the inevitable commoditization of mobile device platforms and services continues to erode certain advantages previously enjoyed by service providers. Mobile network operators (MNOs) have to work harder to maintain a competitive edge. Those who listen to customers and understand their needs and decision points at a deep level will be able to provide the value necessary to attract and retain subscribers. One of the most important differentiators that operators can offer is trust. Closely associated with brand, trust can take years to develop but can be lost in a moment. Subscribers have learned to place a high degree of trust in their service providers, especially in the content they receive such as SMS and MMS messages. Recent scams and malware outbreaks targeting mobile users have begun to erode subscriber trust and established
brands, prompting users to consider alternatives. However, receiving unwanted Spam messages at inappropriate times is a sure way to erode such a trusted relationship and increase costs or even churn.

**Mobile Phones are Personal**

Personal computers have evolved in a relatively open and hostile environment, where new operating systems and applications are immediately tested by hackers seeking to prove their skills or criminals seeking monetary profit. Over the years, this ongoing game of cat and mouse between cybercriminals and security experts has conditioned PC users to a continuous cycle of infection, patching, and updating. Likewise, the widespread use of email has conditioned users to floods of spam and an endless variety of malware and online scams.

By contrast, mobile devices and operator networks have evolved in a far more closed and safer environment, where operators guard their infrastructure and control which subscriber devices are allowed to access it. For years, this ‘walled garden’ approach has allowed service providers to largely shield customers from attackers and outside forces, and has allowed mobile subscribers to develop a more trusting and personal relationship with their mobile devices and the content they receive on them. Users have learned to take the security and privacy for granted, and to trust that the SMS and MMS messages they receive are from legitimate sources.

Recent changes though have started to tear down the ‘walled gardens’ and open up mobiles network to a whole series of new threats and attacks. Included amongst these are:

**Mobile Apps and Trojan Malware**

Each new generation of mobile devices incorporates faster processors, more memory, better displays and more powerful operating systems. This allows developers to create increasingly dynamic apps to improve productivity for business users and enhance consumer’s personal lives.

Unfortunately, an alarming number of subscribers remain unaware that many mobile apps are sharing their personal information with ‘other third-parties’. Information collected by apps can include personal address books, location data, usage patterns, and internet search history. Advertisers frequently collect personal information for use in legitimate ad campaigns, but may also resell user data to less scrupulous spammers and phishers. Even applications like WhatsApp and Facebook are guilty of this, so end users are becoming accustomed to these policies.

Even worse, malware is increasingly finding its way onto mobile phones by masquerading as legitimate apps. Once installed on a subscriber’s mobile phone, these malicious apps can steal contacts, passwords and device information such as the IMEI number without authorization. The malware can even send SMS messages to premium rate numbers resulting in unexpected and costly charges to subscribers. Another tactic employed by malware distributors is the use of a subscriber’s mobile device as a delivery vehicle for spam messages without their knowledge. This is

![Figure 3: Legitimate Mobile App or Malware?](image)
more common in regions that offer unlimited messaging plans. Mobile malware now generates millions of costly service calls for operators every year and tidy profits for attackers.

**Messaging Fraud is Eroding Subscriber Trust and Operator Profits**

SMS and MMS messaging provide an easy way for subscribers to exchange information when voice conversation is not desired, or to share pictures and other multimedia files. In addition, SMS is increasingly being used by businesses for a variety of useful and legitimate reasons including:

- Bank account status and alerts
- Payments by financial institutions
- Coupons and loyalty programs for brands and retailers
- Information for transportation providers
- Opt-in marketing campaigns run by mobile marketing firms
- Password change notification or account verification messages

Criminals are also attracted to this large and growing opportunity, albeit for fraud and theft. Abusive SMS traffic wastes valuable network resources and drives up customer support costs. Malicious SMS messages received though a ‘trusted’ mobile operator can permanently damage subscriber loyalty, increase customer churn, and threaten subscriber adoption of future mobile services. As mobile operators continue to expand revenue through value added services, it becomes increasingly important to provide a secure experience for subscribers. SMS spam and fraud are now affecting the entire mobile ecosystem resulting in degradation of service, operational problems, unnecessary support calls, and loss of revenue for operators. In addition, should operators prove unwilling or unable to control spam and threats, frustrated subscribers may hasten their migration to OTT messaging services.

**The Cloudmark Mobile Security Solution**

It is clear that mobile threats and spam will continue to evolve as mobile attackers become more sophisticated. Just as they have in the personal computer world, attackers will increasingly employ multiple mechanisms and targeted campaigns in order to obtain sensitive subscriber information for monetary gain and identity theft. Regardless of the methods used, all of these attacks will impact an operator’s ability to function and maintain profitability, while eroding subscriber trust and increasing churn. An effective security solution must be able to shut down SMS/MMS spam and fraudulent messaging while detecting and removing malware and threats, before they have a chance to impact mobile devices and subscribers.

The Cloudmark Mobile Security Solution provides the most effective protection against the widest range of mobile threats. As a high-performance, carrier-grade messaging security solution, it provides real-time threat analysis from global sources offering content and subscriber-level policy controls to combat messaging threats. Backed by a unique and powerful combination of patented Advanced Messaging Fingerprinting Technology from the Cloudmark Global Threat Network, the solution can detect all categories of mobile messaging security threats, including their rapidly mutating variants, before they reach the subscriber. The Cloudmark Mobile Security Solution enables participating operators to combat ever-growing
mobile messaging and security threats as they occur, without any service interruption or manual operator involvement.

**Cloudmark Mobile Platform**

The Cloudmark Mobile Platform provides protection against all categories of mobile messaging abuse and threats originating from internal or external mobile networks. Broad visibility into messaging trends enables the creation of effective messaging security policies. The Cloudmark Mobile Platform (CMP) reduces abusive traffic, freeing network and operational resources, and reducing customer complaints related to messaging attacks. Some important CMP features and benefits are detailed below.

**Sender Reputation**

CMP develops ‘reputation profiles’ for individuals and messaging entities based on a variety of information collected over time. This data can include global titles, MSISDNs, IMSIs, message content, header and Cloudmark message ‘fingerprints’. Reputation profiles can be used in combination with protocol and content control policies to create simple, or highly granular message filters. For example, they could be used to limit the number of messages allowed from an individual over a given time period, or to restrict the number of similar messages that can be sent to a given number of recipients.

**Traffic Intelligence**

Cloudmark’s advanced traffic pattern analysis system identifies and blocks attacks in real-time, before they can proliferate on operator networks, while ensuring legitimate messages are properly delivered. By analyzing traffic patterns and scanning billions of messages per day from hundreds of operators worldwide, Cloudmark is able to form robust models of normal and malicious messaging traffic patterns and behavior. Cloudmark can use these models to detect anomalies, block threats, and send alarms and notifications to operators and service centers. For example, high volumes of messages sent from the same source can indicate a threat. Alternatively, low volumes of a particular message sent from many sources could also be malicious.
Message Fingerprinting

Cloudmark has developed a set of intelligent message ‘fingerprinting’ algorithms to identify and track spam, phishing, fraud, malware, and other malicious attacks throughout an operator’s network. Cloudmark’s fingerprinting algorithms work together to identify a variety of threat attributes that might be embedded in a message. For example, they could be used to identify all mutations of a given attack, including changes in content, image, sender, web address, and other attributes.

Message fingerprints can be used to identify and block threats in real-time, before they can affect mobile devices and subscribers. Since Cloudmark’s core fingerprinting technology is format and content agnostic, it detects and mitigates spam, fraud, phishing and malware attacks that arrive in any format including SMS, MMS, RCS, social networking (OTT), email and binary attachments. It can even detect messaging threats and fraud in any language, including those using double-byte characters.
Message Control by Protocol

Operators can control messaging based on protocol attributes and volume patterns over time. For example, administrators can define a policy to throttle or block abusive senders from inside their network and from partner networks, with optional logging of message meta-data or contents for later review. Protocol controls can also be used to monitor and enforce usage policies for value-added service providers and to stop abuse of bulk-sender rights. Alerts can be set to notify administrators based on specific combinations of protocol attributes.

Message Control by Content

CMP scans message content in detail, allowing operators to implement security actions at a granular level. Operators can block messages or alert administrators based on keywords, dictionaries, regular expressions and even specific message elements. CMP also includes the ability to reconstruct multiple message parts of concatenated SMS messages for scanning purposes.

MMS Message Control

CMP provides extensive MMS security capabilities, providing full coverage of the MM1 message channel. It can also scan traffic from other mobile messaging service centers (MMSCs) over MM3 and MM4 interfaces.

Workflow-based Framework

CMP provides fast and flexible policy deployment through a simple workflow-based policy engine. This provides the ability to perform advanced analysis of message content, envelope and source data, including user data header (UDH) information. Such analysis provides comprehensive anti-spam, anti-phishing, and anti-virus filtering, including checking any included phone numbers or URLs inside the messages.

Web-based Management

The CMP administration console allows administrators, operators and messaging abuse teams to easily manage message handling while monitoring threat trends. The convenient web-based interface provides access to data from the Cloudmark Authority automated content filtering service, the Cloudmark Sender Intelligence service, and local data repositories including the Subscriber Preferences Directory. The management console also provides access to system configuration, reports, statistics, and spooled messages.

Customizable Logging and Reporting

Administrators can view statistical data from all CMP nodes within dashboards and reports for how the system is performing. All these are customizable as required by the operator. Simple reporting
interfaces provide a clear view of subscriber issues, threat trends and security effectiveness. Logging and reporting capabilities include:

- Message traffic reports, including the actions taken on messages and reason
- Event reports leveraging counters specified in workflow
- User reported feedback of Spam in the Spam Reporting Services module
- Log files for export to other analysis tools

In addition, the Cloudmark Network Feedback System provides mobile service providers with visibility into filtering performance and customer feedback including daily, weekly, and monthly statistical reporting.

![Custom Messaging Report](image)

**Figure 5: Custom Messaging Report**

**Value-added Services**

CMP frees mobile operator networks from unwanted traffic and improves subscriber trust. This enables operators to offer a variety of value added security services. Several important security-related services made possible by Cloudmark solutions are listed below:

- Corporate Archival and Personal Quarantine – CMP can forward messages to a pre-defined location using TLS encapsulation. This allows operators to offer corporate archival, personal quarantining, and other security-related services.

- Anti-bullying and Anti-sexting – CMP supports natively or can integrate with whitelist and blacklist data sources, enabling operators to offer paid subscriber services such as anti-bullying, anti-sexting, and parental control over message senders.

**Seamless Network Integration**

CMP seamlessly integrates into mobile operator networks and business systems without risk of service disruption. Subscriber policy settings and other information can be leveraged by CMP
message handling. CMP supports integration with LDAP, MySQL and HTTP backends, enabling access to third party data sources and databases. This information could be used to implement subscriber preferences such as anti-bullying blacklists.

**Carrier-class Scalability, Reliability and Performance**

CMP is architected for high scalability and extremely high message throughput, enabling optimization of existing and future mobile network infrastructure. CMP can scale based on a number of transactions per second per node, and can grow utilizing either an N+1 or 2N architecture.

**Cloudmark Sender Intelligence**

Cloudmark Sender Intelligence (CSI) provides operators with valuable data and visibility into mobile sender reputation both within and outside of their network. This intelligence enables real-time action to block messaging threats at the first instance of a new attack, significantly reducing the window of vulnerability available to spammers and phishers.

**Cloudmark Authority**

Cloudmark's content filtering is based on Cloudmark Authority, which combines highly sophisticated and high-performance Advanced Message Fingerprinting technology to analyze the contents of each SMS message. Fingerprints, or data hashes, are generated based on message content and attributes, and matched against Cloudmark's Global Threat Network database of known fraudulent fingerprints. If there is a match, the message is blocked. Authority's content scanning capabilities take into account all information in the message including the sending MSISDN, point code or global title data, message content, message structure, included URLs/phone numbers, UDH and other information. This allows Cloudmark Authority to track commonalities across all malicious messages.

*Figure 6: Cloudmark Authority Content Intelligence Fingerprinting*
Reports from end users, administrators, messaging honeypots and probes are continuously analyzed and new threats are immediately added to the database. Traffic data is analyzed to detect and identify anomalies and suspicious sending patterns. Cloudmark Authority also receives data on the latest known threats from the Cloudmark Global Threat Network every 60 seconds.

**The Cloudmark Global Threat Network**

The Cloudmark Global Threat Network receives real-time threat reports from more than two million subscribers based in 165 countries, and analyzes over 150 million spam and malware reports every month. Members of the Global Threat Network span mobile operator abuse teams, system administrators, automated spam traps, and end users. The latest threats are typically added to the Cloudmark Global Threat Network within minutes of the first attack instance.

**GSMA Spam Reporting Service (SRS)**

To counter the worldwide rise of SMS spam, the GSMA and Cloudmark have collaborated to create the GSMA Spam Reporting Service (SRS). This global initiative enables subscribers to immediately report SMS spam and messaging abuse to their service provider. The provider automatically forwards the reported message to the SRS service where it is analyzed using Cloudmark’s advanced message fingerprinting technology. Cloudmark then corroborates the data and produces an analysis of attacks within the reporting provider’s network. All Cloudmark mobile solutions include the SRS service to provide a feedback mechanism for the end users.
Summary

Subscribers have learned to place a high degree of trust in the services they receive from mobile operators, especially mobile messaging. In order to maintain that trust, operators must deploy effective protections to stop attackers from sending spam and malicious SMS messages to their customers. The Cloudmark Mobile Security Solution provides operators with the technology, tools, and expertise to automatically block the latest mobile messaging attacks, threats and spam - before they can impact networks and subscribers.

The Cloudmark Mobile Platform receives real-time threat intelligence from the Cloudmark Global Threat Network, content filtering information from Cloudmark Authority, reputation data from Cloudmark Sender Intelligence, and spam reports from the GSMA Spam Reporting Service. This comprehensive information provides broad visibility into the latest messaging threats, trends and traffic patterns, enabling rapid creation and deployment of effective security policies. Cloudmark Edge provides outbound traffic security, preventing reputation hijacking and IP address blacklisting. Even rapidly morphing SMS message attacks and zero-day malware outbreaks are quickly identified and stopped. With threats and spam under control, operators can increase revenue and profits by offering new value-added security services to subscribers, while protecting their brand reputation.