market brief

preventing grey routes and the multi-billion dollar threat

rising cost of grey route fraud

The convenience of mobile messaging has brought communication efficiency to billions of consumers worldwide. As is often the case with widely accepted technologies; however, convenience can provide a vulnerable gateway to fraudulent activity. For the communications industry, one of the most prevalent and costly forms of fraud is grey route messaging. It has been estimated by mobile intelligence provider Mobilesquared that the combined amount of industry revenue leakage related to grey route messaging could reach as high as $82.14 billion by 2020.

Grey route messaging occurs when Application-to-Person (A2P) messages are illicitly relayed by fraudsters via channels originally designated for Person-to-Person (P2P) messaging. Grey route activity often occurs undetected and leads to tremendous profit loss for service providers.

the origins of grey route messaging

The roots of grey route messaging can be traced to the early years of wireless communications. As the consumer demand for wireless phones increased, the need to accommodate consumer travel habits grew as well. For consumers traveling with functioning wireless phones, it seemed logical for service providers to provide them with the ability to send and receive messages from any location. As a result, the telecommunications industry implemented a global network roaming system to facilitate seamless and reliable text service, regardless of where a person might be located. The key to this technology was an international signaling system, SS7, dedicated specifically to P2P communications. Initially, regulations for access to SS7 networks were surprisingly lenient, allowing any company that identified itself as an service providers, and could provide an easily obtained Global Title credential, access to the SS7 platform.

Additionally, service providers arranged interconnection agreements with other service providers with whom they frequently exchanged messaging traffic. The agreements often specified that the originating service provider (sender) compensate the terminating service provider (receiver) financially for terminating the transmission. These agreements were often informal and relied heavily on the inherit nature of human text messaging patterns. For example: human messaging interaction often dictates that message recipients will likely reply to the message sender, and, therefore, the two service providers will send and receive approximately the same number of messages in an average messaging exchange. Thus, MNOs felt the overall messaging process generally balanced out, and rather than charging each other a nearly identical amount for terminating messages during an exchange, the two service providers could instead agree to terminate each other's traffic at no charge on SS7 networks using the "bill and keep" policy. This billing policy has served the industry as a digital gentleman's agreement, but combined with the lenient access policy to SS7 networks has also provided a lucrative vulnerability for fraudulent network activity.

preventing grey routes and the multi-billion dollar threat

A2P messaging infests SS7 networks

Fraudsters soon realized that by falsely identifying themselves as legitimate service providers and exploiting the billing vulnerabilities between service providers, they could generate and send thousands of SMS messages via applications to consumers free of charge. For legitimate service providers it was nearly impossible to distinguish fraudulent A2P messages from legitimate P2P messages, and they had no choice but to deliver them both so as to not obstruct legitimate P2P messaging. Since then, A2P messaging has placed an enormous strain on the SS7 platform, forcing service providers to aggressively push back on unauthorized messaging by arbitrarily shutting down suspected A2P messaging.

Fraudsters have since responded to these aggressive service provider tactics by redirecting messages through numerous SS7 points and routes to elude service provider shut downs. The paths for these illicit messages are referred to within the telecom industry as grey routes.

For service providers the biggest challenge in battling grey route messaging continues to be the difficult process of differentiating fraudulent A2P messaging from legitimate P2P messaging, and attempting to surgically remove fraudulent grey route activity from SS7 networks without hindering legitimate consumer messaging traffic.

the need to act

For service providers the need to reduce the profit leakage associated with grey route messaging has never been more crucial. While the messaging industry has previously enjoyed tremendous market growth year after year, recent Over the Top (OTT) messaging applications including WhatsApp®, Facebook® Messenger and LINE™, have claimed substantial market share. This dismal industry forecast has put substantial pressure on service providers to find and maximize overlooked revenue streams. Subsequently, the elimination of grey route messaging has become a top priority for service providers, with 15% of service providers currently utilizing solutions to prevent grey route messaging fraud. Mobilesquared predicts that by 2020, 50% of all service providers will have some level of grey route defense in place.

grey route detection technology

Versatile technology designed to identify, target and eliminate grey routes is currently available, and can be seamlessly installed on a service provider's existing messaging infrastructure. The most recent grey route detection technology performs real-time analysis of individual messages before they enter the network, benefits from sophisticated filtering techniques on SS7 messaging parameters including GT (Global Title), Sender ID, and SMS Center (SMSC), and detects spam and other unwanted content via message text pattern recognition. This advanced technology can also monitor messaging patterns and trends on a large scale, as well as recognize suspicious messaging traffic spikes.

Once fraudulent activity is detected, the anti-fraud system can automatically block incoming messaging traffic. The system can also examine illicit messages and identify the enterprise involved in the messaging. In fact, many enterprises are unaware that their messaging traffic is being sent by an unscrupulous third-party aggregator over grey routes. The enterprise can then be informed that its messaging traffic has been blocked due to improper grey route messaging, which may result in the enterprise switching to a legitimate messaging option that properly monetizes the traffic for the appropriate service provider.

Communications industry leader, iconectiv, has introduced a powerful grey route detection solution for identifying and blocking the most sophisticated grey route fraud activity on service provider networks.

preventing grey routes and the multi-billion dollar threat

defender shield by iconectiv

Defender Shield provides:

Sophisticated real-time analysis—including selective filtering of all A2P messages to ensure effective monitoring of traffic from multiple interconnect links.

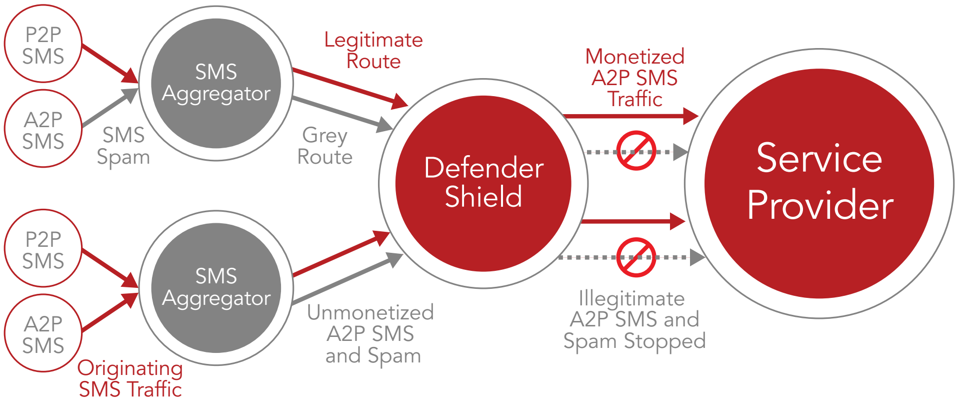
Protection from GSMA fraud cases—including spoofing, GT faking, alphanumeric senders, GT scanning, and HLR dipping.

Grey route detection—analysis of message parameters including (but not limited to) GT, Sender ID, SMSC and/or SMS content monitoring.

Subscriber originating blocking—enabling a subscriber to decide which messages to receive or block.

Full screening control—knowing exactly what is being sent to subscribers and when.

Detailed reporting—extensive drill-down reports on all incoming and outgoing SMS traffic



Defender Shield detects and blocks illegitimate A2P SMS and spam and enables the MNO to monetize its A2P SMS traffic.

Many fraudulent scenarios involve SS7 Protocol Data Unit (PDU) exploitation:

- **SMS spoofing**—messages sent from a fraudster who pretends to be a service provider's roaming subscriber
- **SMS faking**—messages are sent by a fraudster using a fake identity to a service provider's subscribers
- **GT scanning**—thousands of SS7 signaling messages are sent to all Global Title addresses from one service provider in order to find unsecured SMSCs
- **SMS spamming**—unsolicited messages are sent to a service provider's subscribers containing unwanted content

Grey route fraud and related unwanted content impact service providers through:

- Loss of revenue
- Customer complaints
- Customer churn

Sources:
http://www.realwire.com/releases/New-study-says-mobile-operators-must-overcome-risk-averse-A2P-messaging
http://www.netimperative.com/2016/02/how-grey-routes-are-trashing-the-mobile-brand-experience-infographic/

about iconectiv

At iconectiv, we envision a world without boundaries, where the ability to access and exchange information is simple, secure and seamless. Our network and operations management, numbering, registry, fraud and revenue assurance, and messaging solutions enable the interconnection of networks, devices and applications for more than 1,000 customers globally and one billion people every day.

make the connection.

For more information about iconectiv, contact your local account executive, or you can reach us at:

+1 732.699.6800

info@iconectiv.com

www.iconectiv.com

iconectiv®