Mavenir Spam and Fraud Control

Assuring Operator Revenue and A2P Grey Route Monetization

Operators are realizing the scale and potential of A2P (Application to Person) messaging revenues, and how advances in messaging technology will enable them to overcome the dominance of OTT messaging apps. Juniper Research forecasts that A2P messaging revenues will hit $50B globally by 2022[1]. With A2P SMS traffic set to reach 2.7 trillion messages by 2022[2], fraudsters are stealing a large portion of the A2P revenue—approximately $6B annually, according to Juniper. Operators must protect their revenues, their customers, and their reputations from the negative effects of fraud and spam.

Juniper found that grey route A2P traffic accounted for 30 percent of A2P SMS messages in 2017. To help operators avoid revenue loss from grey route fraud, Mavenir has developed a Spam and Fraud Control Solution that is machine-learning based, recognizes fraud in real time, and can cope with advanced firewall bypass techniques. Mavenir enables operators to convert the majority of grey route traffic to white route traffic, which could save billions of dollars on a global basis.

KEY BENEFITS

- Increased A2P messaging revenues
- 3-10x better fraud detection than the top competitors
- Machine-learning technology that outsmarts the fraudsters
- Real-time SIM box detection and blocking
- Automated traffic blocking

"By investing in machine learning, artificial intelligence, we raised the industry performance benchmark for grey route and SIM box message detection by an order of magnitude, placing Mavenir well ahead of the competition."

Ilia Abramov
Leader – Global Security Solutions, Mavenir

Common A2P Revenue Loss Scenarios:

A2P bypass using SIM boxes: An attacker will deploy a set of SIM boxes that leverage unlimited P2P (Person to Person) messaging plans and send massive quantities of A2P messages into the network. This directly impacts A2P revenue, as the attacker is able to terminate messages within the operator network for free. The financial impact depends on the type of traffic terminated, as international A2P is charged at a higher rate than national A2P.

Interconnect imbalance caused by SIM boxes: An imbalance in inter-operator messaging costs normally indicates the existence of fraud. Unsolicited A2P campaigns generated by SIM boxes (via the P2P channel) often terminate outside of the operator's home network. Since there are interconnect agreements related to commercial message termination between national operators, these fraudulent messages represent a direct cost to the originating operator.

[1] A2P Messaging: Opportunities, Competition & Forecasts 2017-2022, Juniper Research, November 2017
[2] Telcos' Opportunities for RCS in the Enterprise, Ovum, October 2017

Termination of incoming A2P traffic through national P2P Interconnect: In this case, due to the difference between A2P pricing and the P2P termination cost, the operator at the terminating end gets hit with fraudulent termination costs. The attacker terminates a large volume of A2P messages from potentially valid MSISDNs that originate from another national network.

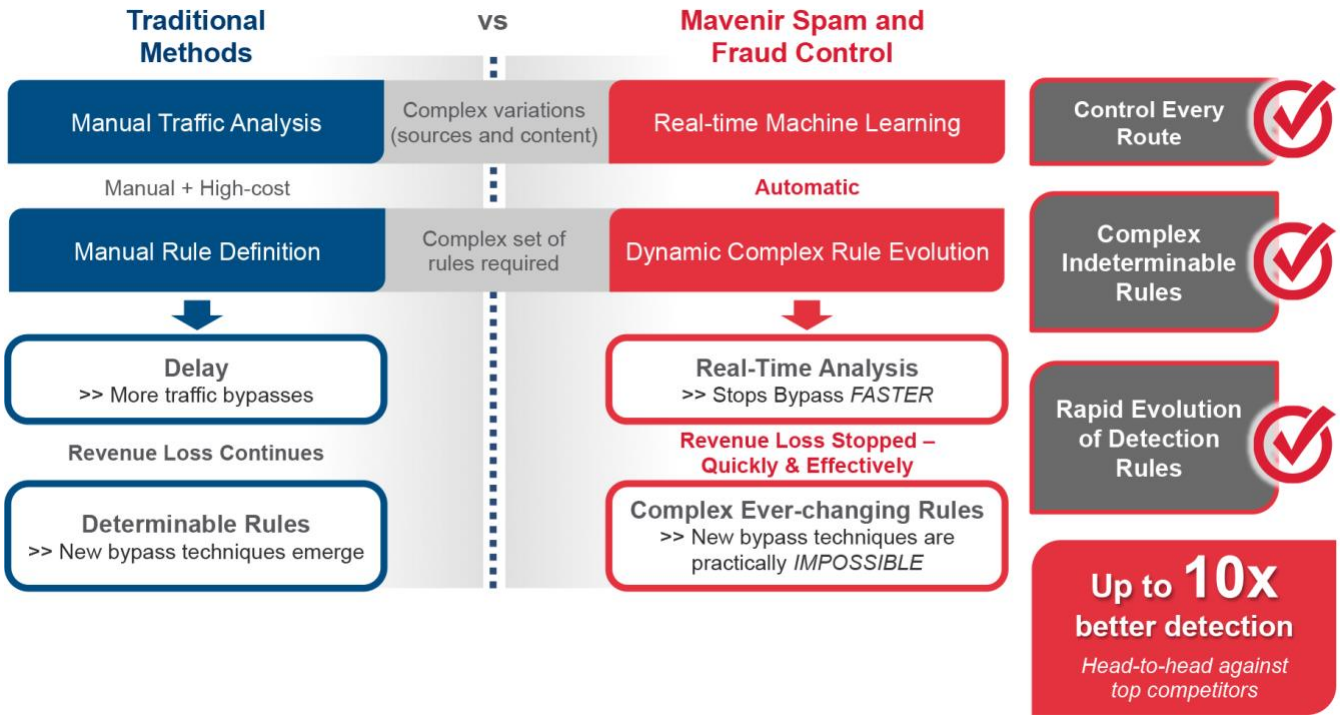
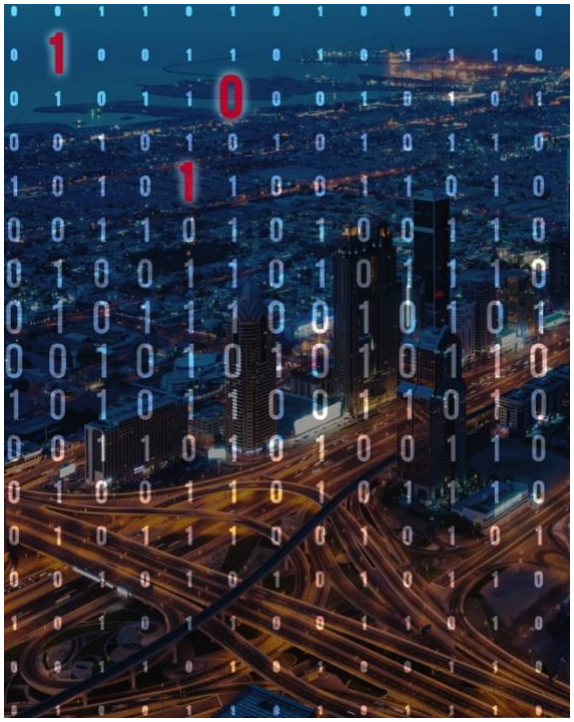


Figure 1: Mavenir Spam and Fraud Control vs. Traditional Fraud Prevention Methods

Mavenir Spam and Fraud Control – Dynamically Adjusts to Changing Threats in Real-Time

Mavenir's Spam and Fraud Control Solution utilizes filtering and detection capabilities that are up to ten times more effective than the competition (Figure 1). The solution utilizes specialized machine-learning techniques that are capable of automatically detecting and selectively blocking sophisticated grey route and SIM box messaging. Mavenir's technology can detect up to eight times more spam-related messages than traditional filtering techniques currently available on the market, including spam received via IP/OTT messaging services.

Solution Description:
Mavenir Spam and Fraud Control



To combat dynamic spam threats, Mavenir's Spam and Fraud Control technology utilizes sophisticated machine-learning algorithms that correlate multiple dimensions of messaging and mobile network properties, while continually monitoring subscriber behavior. The technology's learning process continually adjusts to the constantly changing threat posed by spam to subscribers, and to the operator's brand and reputation. It results in an ever-improving and effective solution that evolves in real-time, as do the characteristics of spam, modifying spam and policy control as appropriate. Mavenir software applies these detection techniques without human intervention, removing any potential delays in the detection process.

Spammers constantly adjust their delivery techniques to beat detection. They utilize SIM farms, which simulate a large quantity of subscribers, and instead of sending massive amounts of messages all at once, they send out bursts of messages, or will interleave various campaigns throughout the day to avoid detection. Identifying and blacklisting spammers can be like finding the proverbial needle in a haystack, except in these cases, the needle keeps moving. Mavenir enables operators to detect and prevent revenue loss scenarios, monetize A2P bypass traffic, and increase control of the messaging network. Mavenir's machine-learning technology ensures timely detection of fraud and A2P bypass regardless of the hackers' techniques, even when they try to adapt to the solution's blocking rules.

There are other solutions in the market today that claim to have comparable detection capabilities; however, they usually have too long a detection delay (>15 minutes) for new campaigns, lack a reliable campaign clustering mechanism, or are based solely on a set of rules that only identify previously known campaigns and scenarios. Fraudsters can easily work around these traditional detection methods, compared to the Mavenir solution which includes campaign clustering algorithms that are extremely efficient and produce zero false positives. All new campaigns are quickly detected, and any filtering bypass techniques are rendered ineffective through a multi-domain, automatic correlation engine.

Mavenir's Spam and Fraud Control Solution can integrate into an operator's existing messaging infrastructure, or Mavenir can provide all of the required elements as a consolidated messaging platform, or only specific elements as required by the operator.

Case Study: Mavenir Helped Telefonica Increase Revenue by Preventing Spam and Monetizing Grey Routes

To address their A2P messaging concerns, Telefonica turned to Mavenir, not only for their industry-leading Spam and Fraud Control Solution, but because they needed a trusted solution provider to partner with. They asked Mavenir to analyze their networks and make strategic fraud prevention decisions without compromising the quality of their overall messaging services.

Mavenir audited Telefonica's Latin American networks to identify messaging revenue leakage. Telefonica was quite surprised by Mavenir's findings: In one country, 70% of the messaging traffic was generated by only .02% of their subscriber base, and these messages were sent to a massive amount of destinations. In contrast, 99% of the subscribers sent fewer than 150 messages to no more than 50 different users per month. The other regions demonstrated similar messaging patterns.

In the final analysis, Mavenir estimated that Telefonica was losing $18M annually due to fraudulent A2P messaging. It was obvious that spammers were sending A2P messages disguised as P2P messages (grey routes), and probably using SIM farms to generate millions of illegal messages across the network.

One windfall benefit Telefonica never anticipated relates to their monthly interconnection fees – the money they pay to or receive from other carriers for terminating messages. Before deploying the Mavenir solution, they experienced regular monthly interconnection fee deficits, yet after the first month of deployment, they showed a profit of $US3M.

ORGANIZATION SNAPSHOT

- **Company**: Telefonica Hispanoamerica
- **Location:** Latin America
- **Employees:** 30,790
- **Objective:** Identify and stop fraudulent A2P SMS messaging costing $18M annually
- **Solution:** Mavenir Fraud and Spam Control Solution

IMPACT

- 20% increase in annual messaging revenue after first three months of Mavenir solution deployment
- 9 million fraudulent messages blocked after the first day of deployment
- 20,000 users blacklisted after the first day of deployment (each sending an average of 180,000 fraudulent messages per day)
- $3M monthly increase in revenue from interconnection fees
- 40M fraudulent messages blocked monthly

"Mavenir made audits of all our networks to identify types of fraud; they estimated we were losing more than $18M per year to grey routes in the region."

Leonardo Hilario
Planning and Project Manager, Telefonica

Summary

Mavenir's Spam and Fraud Control Solution enables mobile operators to detect and prevent revenue loss scenarios, monetize A2P bypass traffic, and increase control of their messaging network. Mavenir's unique machine-learning technology ensures the timely detection of messaging fraud and A2P bypass, regardless of the attackers' techniques, even when they are attempting to adapt to potential blocking rules.

Mavenir enables operators to protect their revenues, their customers, and their reputations from the negative effects of fraud and spam, equipping them to dominate the competitive A2P messaging market.

Rev01-18-02-24