

Bypass Fraud

At a glance

Fraud remains a big challenge for the telecommunications sector. Fraud is persistent, invasive and harms customers and institutions alike. Fraud threatens to compromise not just business results but also customer relationships and brand perception in the market.

As the shift to cloud-based services increases, fraud management capabilities can be delivered as hosted services to help drive more operational efficiencies and to improve business agility. Mobileum RAID.Cloud combines the power of a reliable fraud management solution with the benefits of a hosted, cloud-based deployment model, while still delivering event processing, monitoring, rules management and case management for roaming files.

Around the world, more than 40 organizations look to Mobileum Fraud Management solutions for world-class capabilities to prevent and detect telecom fraud across

Bypass Fraud

Bypass Fraud is the most damaging and costly type of fraud, which effects in particular countries where the cost of terminating international calls is much higher than a national call, and also in countries where international gateways are owned exclusively by government carriers. This fraud type has several scopes and can be recognized by the most common behaviors:

- “Grey Routing” are arrangements where during the route of a call an illegal action is taken such that even though both sides of the call look legitimate, for the sending operator it may look like an international call, for the receiving operator it may look like a domestic call and the settlement is done as if it were a local call;
- “Landing Fraud” occurs when a call is “landed” on a carrier’s network in a way that avoids toll charges. This is accomplished by making the traffic appear to have originated locally, or within the carrier’s network;
- “International Simple Resale” involves landing off-net calls onto an operator’s network but avoiding the international gateway to avoid the international interconnect charges;
- “SIM Boxes” involves several SIM cards (pre or postpaid which are harder to be identified) being used to generate the maximum concurrent mobile calls possible;



a variety of fraud types, technology implementation or telecom products – including mobile, fixed and new services which are driving a step change in the telecommunications industry.

When you successfully protect customers from fraud, their satisfaction soars. Only Mobileum delivers fraud protection with a holistic view.

Bypass fraud is the exploitation of immobile to mobile gateway equipment, typically called SIM boxes, to hijack inbound international calls while transferring them over Voice over Internet Protocol (VoIP) to the mobile network. As a result of this action, it re-injects the call back into the mobile network, thus terminating as a local call at the destination, creating a divergence which makes the carrier operators lose their call termination charges.

RAID.Cloud Bypass Fraud Application delivers an out-of-the-box solution to identify and recommend actions to stop these abnormal behaviors, delivering a service based on multiple layers of tracking, subscription-based access and security mechanisms to confirm Bypass Fraud MSISDN cases. Once detected, the application can then initiate a dedicated and combined analysis to uncover the associated numbers.



mobileum

Action driven by intelligence

Key benefits/Results

- Decrease revenue loss due to call redirection, service inaccessibility and missing call backs;
- Increase customer satisfaction by maintaining service accessibility and quality standards;
- Eliminate possible illegal national/personal security intrusions and route bypassing;
- Eliminate hardware investment in tracking bypass equipment;
- Shorter time to market, register and start;
- Subscribe one or more apps and built your customized Fraud Management solution according to your own needs and budget;

Key features

- Next-generation services configured out-of-the-box to provide full coverage of Bypass Fraud;
- Exceptions list (black and white lists of numbers, call types, etc.) to reduce the amount of false positives;
- Profile matching of fraudulent MSISDN across existing active subscriber base;
- Dealer identification to help tracing back the involvement of a dealer in supplying bulk SIM Cards for use in Bypass Fraud;
- B Number analysis to uncover the common A numbers which are part of the Bypass Fraud;
- Route Analysis to identify the traffic origination (country) for more focused reporting;
- IMEI analysis to identify the related connections from the equipment used to conduct Bypass Fraud;
- Alarm management with a graphical dashboard and insightful email notifications, to allow you to have instant awareness of all possible fraud types and behaviors with recommended mitigations.

- Detection engines that continually evolve based on the latest fraud trends;
- Continuous upgrades to upcoming GSMA recommendations;

Critical differentiators

- RAID.Cloud combines ease of use with the accuracy of a leading fraud management software, all with the convenience of a cloud-based service.
- RAID.Cloud fraud management solution requires no hardware or software to buy, install, maintain or update. Access to applications is easy; you just need an internet connection.
- Our solution provides access to data from any networked device while making it easier to manage privileges, monitor data use and ensure everyone sees the same information at the same time.
- RAID.Cloud can also help accelerate deployment time as well as reduce the ongoing costs associated with managing a traditional on-premise application.
- Combining the proven capabilities of our on-premise deployments with the cloud approach, Mobileum can leverage on how to help Communication Service Providers (CSPs) maintain fraud management agility and operational efficiency while simultaneously reducing fraud exposure to new fraud types threats.



About Mobileum

Mobileum is a leading provider of analytics solutions for the Telecom industry. More than 750 communications providers rely on Mobileum Active Intelligence platform to increase roaming revenues, improve network security, minimize fraud and risk, and optimize business operations. With a strong record of innovation, Mobileum is recognized for its ability to extract deep network and customer insights and to convert them into real-time actions that increase revenue, improve customer experience and reduce costs. Headquartered in Silicon Valley, Mobileum has global offices in Argentina, Dubai, Hong Kong, India, Portugal, Singapore and UK.

Learn more in www.mobileum.com
and follow [@MobileumInc](https://twitter.com/MobileumInc) on Twitter.

MOBILEUM, INC.
20813 Stevens Creek
Boulevard, Ste. 200
Cupertino, CA 95014 USA

Phone: +1-408-844-6600
Fax: +1-408-252-1566

mobileum.com