



# Zero-Rated Fraud Management

Get paid fairly by detecting and mitigating a range of zero-rating fraud techniques



Sandvine's application and network intelligence capabilities can be

leveraged in 5G core and edge environments, delivering critical contextual and slice awareness to feed new service creation and strengthening a service provider's position in the 5G value chain for consumer and enterprise markets.

## ZERO-RATED FRAUD MANAGEMENT DELIVERS:

### Zero-Rating Fraud Prevention

Detects and prevents attempted fraud leveraging zero-rating exploits

### Prevention of Unauthorized Access

Restricts specific applications that are not allowed with certain plans

### Terms and Conditions Fraud Prevention

Blocks attempted circumvention of terms and conditions that can lead to network abuse (e.g., tethering or line sharing)

### MARKET OVERVIEW

Service providers are challenged with attracting new users and improving the trend of declining ARPU. In order to solve these problems and grow market share in a fiercely competitive landscape, service providers must innovate their service offerings to gain new customers and retain existing ones.

One popular tool is zero-rating, as it allows service providers to achieve market differentiation and offer value to attract new users, as well as retain existing ones. However, the use of zero-rating creates a new and attractive surface for unscrupulous users wanting to exploit weaknesses in the network and bypass payment for the services offered, which directly impacts the service providers' revenue and the brand perception.

To successfully implement zero-rating, service providers need to be aware of the cost of zero-rating – fraud – and apply careful planning and market awareness to ensure they get paid for the services they deliver. Specifically, service providers need to be able to detect and act to prevent various methods of zero-rated fraud. Misclassification of traffic and unmanaged fraudulent behavior can have heavy financial consequences due to charging errors, unnecessary capacity expansions, and deteriorating quality of experience for regular users.

There are a variety of techniques used in zero-rated fraud, such as HTTP header injection, domain fronting, and DNS spoofing, but data fraud is not limited to zero-rating.

### Additional target areas for fraud:

- Subscription mismatch between IT and network (e.g., prepaid subscriber connecting as postpaid)
- Abuse of commercial terms and conditions for plans (e.g., tethering restriction)
- Billing charges for events (e.g., ringtones or music on demand)
- Access to unauthorized content

The challenge for service providers is not isolated to only detecting fraudulent behavior, but also taking the right action and preventing abusive usage, not only targeting zero-rating practices, but in the network overall to protect valuable revenue.



Sandvine's frequently updated signature library ensures accurate identification of attempted data fraud and enables active management to prevent fraud

### USE CASE OVERVIEW

Sandvine's Zero-Rated Fraud Management use case uses the ANI Classification Engine to deliver superior traffic classification and policy enforcement to strengthen service providers' defense towards fraudulent behavior in the network. The right policy enforcement empowers the right response to fraud when detected and, with behavioral analysis, heuristics, and machine learning, prevent future fraud as well as potentially recover lost revenue even if the traffic is encrypted.

Sandvine has partnerships with OTT application providers to ensure that traffic associated with these applications is classified correctly through the Sandvine Gateway API. In the case of sponsored data opportunities, this API has the ability to build trust between service providers and content owners, minimizing billing errors. With correct classification and billing, service providers can confidently implement zero-rating and take advantage of sponsored data opportunities as they can mitigate revenue loss associated with fraud, misclassification, or billing errors.

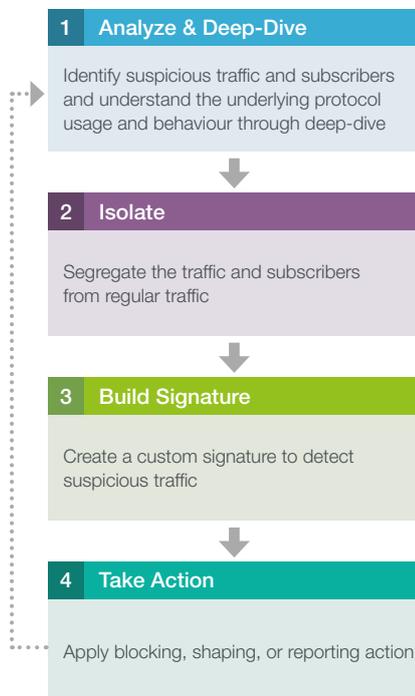
**Sandvine's Zero-Rated Fraud Management delivers these key capabilities to any zero-rating data practice:**

- Advanced traffic classification powered by machine learning, heuristics, and behavioral analysis, to deliver accurate application and traffic identification, even for encrypted traffic
- Rich policy enforcement options to empower service providers to respond appropriately when fraud is detected, prevent fraud, and potentially recover lost revenue
- Advanced reporting and analytics that provide insight into the prevalence of data fraud and the impact of management policies
- Sandvine Gateway API for partnerships with OTT and application providers for ensuring accurate traffic identification for high-profile OTT traffic

Sandvine's rich visibility and reporting visualization ensures that the service provider can see the scope of the fraud that is occurring on their network, and then determine the appropriate actions to take, including drilling down to determine the exact techniques being attempted to commit data fraud.

**Zero-Rated Fraud Management enables service providers to detect and act on fraudulent behavior occurring inside the network. With traffic visibility, fraudulent users that have abused service agreements can be moved to a higher volume plan and charged for their usage, and service providers can recover valuable revenue.**

#### Data Fraud Management Lifecycle



### ABOUT SANDVINE

Sandvine's cloud-based Application and Network Intelligence portfolio helps customers deliver high quality, optimized experiences to consumers and enterprises. Customers use our solutions to analyze, optimize, and monetize application experiences using contextual machine learning-based insights and real-time actions. Market-leading classification of more than 95% of traffic across mobile and fixed networks by user, application, device, and location creates uniquely rich, real-time data that significantly enhances interactions between users and applications and drives revenues. For more information visit <http://www.sandvine.com> or follow Sandvine on Twitter @Sandvine.



**USA**  
5800 Granite Parkway  
Suite 170  
Plano, TX 75024  
USA

**EUROPE**  
Svärdfiskgatan 4  
432 40 Varberg,  
Halland  
Sweden  
T. +46 340.48 38 00

**CANADA**  
410 Albert Street,  
Suite 201, Waterloo,  
Ontario N2L 3V3,  
Canada  
T. +1 519.880.2600

**ASIA**  
RMZ Ecoworld,  
Building-1, Ground Floor,  
East Wing Devarabeesanahalli,  
Bellandur, Outer Ring Road,  
Bangalore 560103, India  
T. +91 80677.43333

Copyright ©2022 Sandvine Corporation. All rights reserved. Any unauthorized reproduction prohibited. All other trademarks are the property of their respective owners.

This documentation, including all documentation incorporated by reference herein such as documentation provided or made available on the Sandvine website, are provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Sandvine Corporation and its affiliated companies ("Sandvine"), and Sandvine assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect Sandvine proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of Sandvine technology in generalized terms. Sandvine reserves the right to periodically change information that is contained in this documentation; however, Sandvine makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.