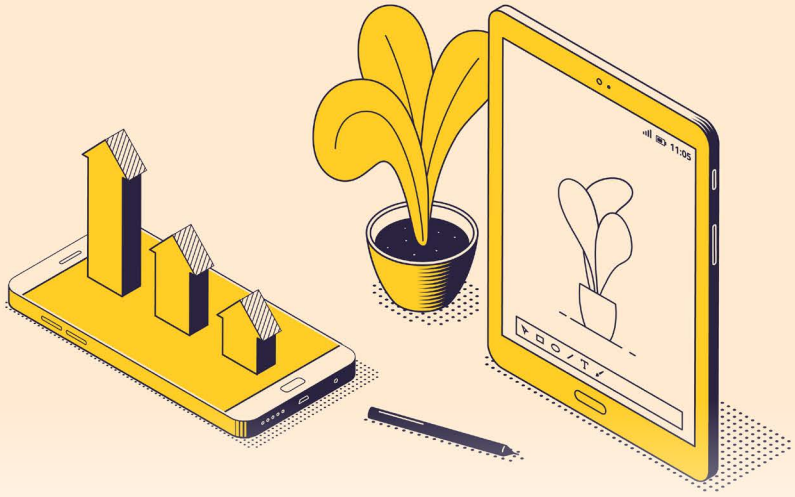
CASE STUDY



# Bad Debt & Fraud

## How a leading Russian mobile operator is successfully tackling the issues

Russia is one of the fastest-growing mobile markets in the world. At the end of 2017, the number of mobile subscribers in the Russian Commonwealth exceeded 230 million, with a corresponding penetration rate of 80% (source GSMA).

> **With the advent of Optimus, Bad Debt in VEON has dropped from 2.8% to 1.3%**

Such exponential growth often leaves the door open to fraudsters - it is not uncommon for operators to concentrate on building market share, whilst neglecting to put effective fraud management processes in place until it is too late.

In this case study, we examine how Russian mobile operator, VEON, successfully implemented a fraud management system which not only enables them to manage fraud in the present, but will also carry them through to the future, effectively dealing with subscriber growth alongside new and evolving fraud types.

## VEON Russia – A case in point

Founded in 1993, VEON (formely VimpelCom) is one of Eastern Europe's leading providers of wireless telecommunication services. The VEON group includes cellular companies operating in Russia, Kazakhstan, Ukraine, Uzbekistan, Tajikistan, Georgia and Armenia. VEON is a leading global provider of connectivity and internet services. Present in some of the world's most dynamic markets, VEON provides more than 210 million customers with voice, fixed broadband, data and digital services. These figures are growing daily due to rapid expansion in the Russian market.

## The fraud problem

VEON saw its GSM 900/1800 network launch and sales channel growth through dealers and points of sale, with the focus being on pre-paid service offering.

The main types of fraud that VEON was experiencing were subscription fraud, roaming, dealer fraud and handset subsidy losses.

VEON had no automated responses in place to manage fraud: efforts were being carried out manually and were further hampered by the fact that the persons tasked with fraud management worked within several different departments.

> **Bad Debt reduction from 2.8% to 1.3%**

Therefore, the operator commenced its Fraud Reduction Project. A cross-functional team, comprising 11 employees, was formed and tasked with the development of in-house reports (high usage, roaming, etc.), a credit limit sub-system and a reward scheme for new dealers. As a result, fraud losses were halved and the project deemed a success. However, VEON recognized that fraud is a moving target and that they could not afford to sit on their laurels.

The next year, a fraud review was conducted, which highlighted more than 80 major issues. A new fraud management approach was established, which comprised maximizing fraud protection, minimizing costs and focusing on the areas of greatest potential loss. The fraud management functions were centralized and a new fraud management department established.

## FMS selection process

Following the review, VEON issued an RFP for a new fraud management solution. The vendor selection criteria were as follows:

## Functionality

**Fraud types detected**: The system should be able to detect all traditional fraud scenerios as well subscription, technical, internal, etc.

**Detection techniques**: The system should incorporate rules/thresholds with more advanced technologies such as neural networks

**Data streams**: The system should be able to process customer data, voice CDRs, SMS, TAP, GPRS, etc. Flexibility: The system should be a tool, not a "black box", full visibility of the detection, analysis and management must be available

**Processing CDR data**: The system should be able to process CDR data in real time to produce fraud tickets as soon as the fraud occurred

**Customer data**: Ability to store important customer data and use that to enhance the quality and accuracy of tickets generated

As well as the above factors, there were also some important underlying requisites from VEON.

## Scalability

The fraud management system should be highly scalable - VEON's growth projections in the forthcoming years were extremely high and the system needed to be able to cope with dramatically increased subscribers and higher volumes of CDR throughput.

Optimus from Neural Technologies is scalable to ensure it expands to accommodate VEON's subscriber growth and service predictions.

The system runs on a Sun / Oracle platform, which is VEON's corporate standard.

Optimus' security parameters are highly configurable, permitting the setting of users/groups/modules individual or group access rights. The system audit logs ensure that every action is monitored and recorded.

## Vendor experience

The vendor needed to demonstrate experience in

installing fraud management systems in similar environments around the world and prove that statements given within the RFP repsonse could be substantiated.

### Support in Russia

The vendor needed to demonstrate that a structured support service was in place to ensure positive interaction with VEON and comprehensive support throughout the implementation process.

### IT standards, security, recoverability, 7x24

The vendor had to ensure that the system was capable of running at maximum throughput 24 hours a day, 7 days a week. The system should comply with security standards laid down by VEON, and have a minimum downtime period during maintenance or upgrades.

### Financial considerations

The vendor needed to present a commercial offer and ROI model that could be proven in the telecommunications environment and to demonstrate willingness to ensure that the system would be implemented and functioning to VEON's exact requirements.

## FMS solution selection – Optimus

Neural Technologies was selected as VEON's chosen supplier after a vigorous and intensive analysis process.

The reasons VEON gave for Neural Technologies selection were based upon a variety of competences:

### Vendor experience

Neural Technologies possesed a qualified professional team who provide continuous improvement (monitoring, analysis, updates, consultancy).
The initial fraud configuration template was quickly adjusted to satisfy VEON's own requirements.

### Support in Russia

Neural Technologies' secure remote access facility (VPN), assured VEON that the system could be monitored day or night by skilled professional personnel who knew and understood the system.

As well as this, Neural Technologies provided an online support website to allow VEON full visibility, tracking and resolution of issues raised.

### Financial considerations

Neural Technologies offered VEON its unique Price Performance model, that ensures both vendor and customer shared the risk of installation and ongoing performance of the system. This gave VEON confidence in the solution, because should it fail to meet performance criteria set out in the joint agreement, VEON would not be required to pay.

### Functionality

The system proved in real-life scenarios that all fraud types could be detected and analyzed: Subscription, Roaming, High Usage, Call Selling, Technical, Hacking, Tumbling, Cloning, Internal etc., plus other revenue leakages.

The system utilized both traditional and advanced detection techniques that were proven to work:

- Traditional, i.e. rules/thresholds/black lists
- Advanced usage and destination profiling
- Neural predictive analytical models

The system has the ability to accept any data streams (online or offline feed). Critically, customer data can be used as part of the analysis process – contracts, price plans, services, charges, payments, etc., in addition to EDRs (Event Data Records) such as voice, SMS, TAP, prepaid balance change events, log files, etc.

> **Improved accuracy of fraud identification - average ratio of 'good'/'bad' tickets is more than 60%**

## Flexibility

VEON were impressed with Optimus' Fraud Configuration Manager. Not present within any other fraud solution, this unique module, which sits within a user friendly GUI, enables VEON to:

- Change/add rules, thresholds, special lists, etc.
- Change existing or add new data streams
- Configure a personalized user interface: views, fields, colour coding, etc.
- Develop/update/implement scorecards whenever required

## The Results

VEON are delighted with the results that Optimus is achieving for them - the operator cites the main ones as being:

- Fraud detection time and accuracy
- Faster identification of fraud - Optimus is working with EDRs (Event Data Records) in online mode
- Highlighting of fradulent or credit risk subscribers upon application, i.e. before they reach the billing stage- therefore fraud detected much faster
- Improved accuracy of fraud identification - average ratio of "good/bad" tickets is more than 60%

## Business processes improvement

Eliminates huge amount of manual work in the Fraud Management Department. Management reports are available much faster, enabling rapid decision making.

## Scalability

The system has proven it can grow with VEON's subscriber growth predictions. When the system was first installed, VEON's Russia subscriber base was 2.5 million (17 million EDRs per day). After two years it stood at 47.7 million (225.3 million EDRs per day).

## Next steps

Regular teleconferences take place with users and managers to ensure satisfaction and ensure that the system is functioning as required. Periodic visits are undertaken to ensure the working relationship between Neural Technologies and VEON is maintained.

VEON's future plans are centered around expanding Optimus to cover not only their core business in Moscow, but also to cover the whole of Russia from St. Petersburg to Vladivostok. In addition, they want to use Optimus to monitor other areas of their network such as GPRS, MMS, IT Systems, SS7 probes and their D-AMPS network in Moscow.

VEON also plan to develop neural predictive analytical models for each market segment, in order to expand the use of Optimus in the wider areas of revenue assurance.