A Market Research Report

Telecom Fraud Management Services, Software & Strategies

Vendor Profile:

October 2015

Technology Research Institute (TRI)
1245 N. Rocky Mountain Drive
Effort of the Poconos, PA 18330

Tel: 570–620-2320

www.technology-research.com

Copyright 2015 Technology Research Institute
1. COMPANY ACTIVITIES

a. Corporate Mission

WeDo Technologies is a leader in Enterprise Business Assurance, providing software and expert consultancy, to analyse large quantities of data to protect revenue, save costs, and minimize operational or business inefficiencies. The company employs more than 500 people.

WeDo Technologies is owned by the Sonae Group, the largest non-financial Portuguese industry group with € 5.7 billion in revenue and more than 43,000 employees in 18 countries. The company is active in Retail, Real Estate, Telecommunications, Media, and Forestry industries.

b. Customers

WeDo has more than 180 telecom operators from 90+ countries as clients across the domains of revenue assurance, fraud, and cost assurance lines. TRI estimates about 10% of WeDo’s business is serving the business assurance and auditing needs of firms in the retail, energy, insurance, and healthcare industries.

Here is a list of key telecom operators that WeDo serves. About 80% of the shown telecoms have the WeDo fraud management solution:

**Asia Pacific**
- Etisalat Afghanistan
- Mobilink Pakistan
- TIME dotCom Berhad
- XL Axiata - Indonesia
- Vodafone Hutchison Australia
- Malaysia

**The Americas**
- Cablemás - Mexico
- Cablevision Mexico
- Cablevision Monterrey/TVI
- Claro Ecuador (Porta)
- Nuvetel (Viva) Bolivia
- Cricket Communications - USA
- Orange Dominica
- Mexico
- Republic
- TNSI/Roamex - USA
- U.S. Cellular

**Europe – EU+**
- France Telecom
- Orange Business Svc France
- UPC Netherlands
- 3 UK
- Vodafone Portugal
- Vodafone Spain
Europe, Middle East & Africa

Azerfon Azerbaijan  Côte d'Ivoire Telecom  Orange Niger
Orange Slovakia  Maroc Telecom  STC Saudi Arabia
UPC Hungary  Mobinil - Egypt  VIVA Bahrain
Turkcell  Nawras Oman  Etisalat Egypt
Vodafone Turkey  Orange Cameroon  Etisalat UAE
Unitel Angola  Orange Ivory Coast  Vodafone Egypt
Asiacell - Iraq  Orange Madagascar  Vodafone Qatar

2. TRI'S ANALYSIS

Background of WeDo Technologies

WeDo Technologies has the largest market share of software vendors serving telecom business assurance -- the combined domains of revenue assurance, fraud management, and partner cost management.

In 2001 WeDo Technologies was born as a spinoff of Optimus, a mobile operator in Portugal. Actually WeDo Technologies’ CEO is the former CIO of Optimus. The company started as a systems integrator and IT consulting firm, and to this day some people in southern Europe still think of WeDo Technologies as an SI. Yet in recent years, probably 90% of its business has shifted to software and professional services.

From the beginning, the relationship with its parent, Optimus, was key because it enabled WeDo Technologies to launch in the business with a captive customer, although the percent of total business WeDo Technologies does with its parent has steadily declined over the years and TRI estimates was about 5% in 2014.

The first big break for WeDo Technologies came in 2001 when it won a very big contract with Brazil’s Oi (the first GSM operator in Brazil), part of the Telemar Group. At that time Oi acquired WeDo’s systems in roaming management, incentives management and collections. And it was Oi that in 2002 first challenged WeDo Technologies to develop its RA tool, RAID. Oi was also the firm that insisted upon a commercial product, not an in-house tool.

The Orange Group, in particular, has an exclusive relationship with WeDo Technologies in revenue assurance. The Vimpelcom Group (Beeline) based in Russia is another key group account. Vimpelcom recently purchased part of the Orascom Group (based in Egypt), with whom WeDo Technologies had already established a strong relationship since 2005/2006.

The CAPE Technologies acquisition in 2007 brought in some important Vodafone Group accounts, but WeDo Technologies has also added to the penetration of that strategic customer. Another key partner is the Digicel Group, that operates out of Jamaica covering 32 markets in the Caribbean, Central America and the Pacific.
WeDo Differentiators

After a discussion with WeDo’s product management team, here’s TRI’s analysis of what makes WeDo Technologies tick – across its business, and particularly in fraud management.

RAID: A Commitment to Powerful, User-Specific Enterprise Software

WeDo came into the fraud management domain relatively late in the game. So to gain any market share, it knew it had to be disruptive and offer something different. The path it chose was to improve the usability of FMS software. This strategy is evident in several design choices the company has made to its RAID product suite:

- **Adopting Interface Ideas from Popular Analytics Software** – Rather than reinvent the wheel in GUIs, WeDo follows de facto standards in enterprise software. Since many financial departments use tools like Tableau and QlickView to transform data columns into dashboards, WeDo has put a similar capability into RAID. Likewise, many fraud investigators are comfortable with Excel, so WeDo accommodates them by enabling Excel-like mashups of data columns.

- **Boosting the Collaborative Power of the Tool** – Another RAID design goal is to help its customers solve assurance problems across their entire companies, not just among Revenue Assurance and FM staff members. Fraud management staff members, for instance, need a lot of contact with many other areas of the company. So it designed the platform to enable sharing and views by people with many different job titles within their company.

- **A DIY Interface that Doesn’t Require IT Expertise** – WeDo is a big champion of Do It Yourself (DIY) IT. While enabling less IT-savvy users to use RAID requires a big investment on WeDo’s part, they feel it’s the wave of the future. So WeDo is busy creating interfaces that provide helpful advice and recommendations, as well as visual drag and drop tools that require no coding knowledge.

In the fraud area, the RAID interface guides the user to visually create new fraud detection engines – particularly useful for non-traditional fraud analysts who want to access the FMS. For example, experts with deep law enforcement or security domain knowledge can get great benefit from an FMS, but they generally have zero knowledge of SQL – and they don’t have time to learn.

So WeDo provides a path for those experts to use the FMS and the broader enterprise assurance platform. RAID ETL empowers users to manage Hadoop data without writing code. It’s simple to load data from relational data sources or RAID data sets to and from Hadoop – making it easy to make big-data ready and available for reports, visualizations or advanced analytics during fraud investigation.

- **User Specific Dashboards** -- Traditionally, revenue assurance and fraud software has been built around a standard dashboard, standard reconciliation approach, standard reports, and standard business rules you configure for the entire organization. And normally the user had to get help to fine-tune those standard capabilities for personal use.

With RAID:Telecom each user now has his own "cockpit" with his own "business sensors" and rules to look at the revenue streams that are highly relevant to the particular user. And more than that: if a particular user develops a more efficient work environment on her own,
she can publish that as a template so her colleagues can use it as well -- and fully customize it on any device from smartphone to desktop workstation.

- **Making the ETL of New Data Source more Visual** – Another aspect of WeDo’s DIY system is to make it easier to input into RAID new data feeds, including structured and unstructured big data.

  WeDo’s new visual ETL feature is built-in: it does not rely on any third party system. What’s more, the system becomes completely agnostic to the data sources it uses.

  The whole point of a visual ETL is to take away the user’s frustration. The tool can not only process lots of data, if you need to integrate with Hadoop, you don’t have to call the IT department and wait 2 months to get some help.

**FMS: Broad Fraud Detection Capability & Complete User Control**

WeDo’s fraud management philosophy is to give lots of power to the individual auditor, investigator, or analyst. Rather than deliver a “black box” system where the logic is hidden from the user, WeDo enables the user to gain full control and evolve the system himself and directly change, say, the detection rules or any parameter in the system. This allows CSPs to use the same system to protect against International Revenue Share Fraud or SIM Cloning and at the same time be protected from emerging fraud threats in areas such as SS7 signaling exploitation.

From time to time, individual fraud threats will challenge the ability of the FMS to keep up. For instance, advanced stealth techniques employed by fraudsters are making it harder to detect SIM box bypass.

To make its FMS better in the SIM box battle, WeDo is supplementing its traditional call volume, duration and cell dispersion detection with advanced analytics. For instance, RAID uses analytics to detect where there’s an 80% match with an existing rule, allowing the user to identify those cases and turn the deviation into a new rule.

And the RAID solution is also used in a “hybrid way” to take test call generator intelligence about gray routes to multiply the ability of operators to detect SIM box bypass.

**Taking Fraud Management Lessons from Other Industries**

The importance of improving usability of RAID was reinforced for WeDo when it started providing solutions to other industries.

Though only 10% of WeDo’s revenues come from outside the telecom industry, the company is pushing to broaden the cross-industry appeal for its solutions. For instance, at an insurance company in Latin America, RAID was used to:

- Help the fraud department redesign their internal processes to create a better workflow;
- Decrease fraud department costs, saving an average $1 million a month in expenses; and,
- Detect, analyze and manage more than 7,000 fraud attempts in the past year, helping to avoid $20 million in fraud indemnity losses.
This work in other industries has also provided valuable WeDo with valuable insights on how to best tailor its solutions. For instance, they discovered that outside of telecom, IT specialists don’t generally work in auditing and fraud assurance. In the retail industry, for example, it is the financial analysts and internal audit teams who manage the data themselves. Retail firms generally don’t have a dedicated fraud team either.

An expert in fraud or internal audit has great domain knowledge that’s hard to duplicate. So the way to add value is to bring tools that allow these experts to better leverage information technology in their special domains. And that usually means giving them an easy means to assemble data from various sources as they try to resolve various cases.

**Insider & Dealer Fraud Investigations**

As the telecom industry gets steadily better at controlling IRSF and other fraud threats, it increases the tendency for fraudsters to commit fraud with the help of insiders or the dealers who sell the carrier’s services.

Well, the flexible interface and data source integration capabilities of RAID are well-suited for helping investigators of insider or dealer fraud problems. And certain operators are taking advantage of its capabilities.

At one WeDo customer, for instance, 80% of the controls in place are related to dealer activity. In fact, the purchase of RAID was made after the operator’s internal audit found a huge fraud occurring on the dealer network side.

The RAID implementation monitors: subscription sign-up activity of the agents; commissions paid; and call backs to agents. Even service activations and service upgrades are tracked.

**Expanding RAID into Other Enterprise Processes**

These days WeDo is pushing the use of RAID to telco business functions way beyond RA and fraud analysis.

In particular, they are reaching out to telecom CFO organizations and auditing teams. For instance, WeDo has introduced a balanced scorecard -- fully compliant with the Kaplan methodology – that allows a CFO to use a balanced scorecard to drill down into business dimension to look at the specific revenue streams and get more details on problems being experienced in near real-time.

The strategy is to make an operational risk policy more meaningful across the organization through real-time monitoring – and minimizing surprises.

Taking a cue from the way SAP sells enterprise packages for Human Resources, Finance, etc, WeDo offers similar solutions for the auditing of functions such as procurement assurance, equipment handling assurance, and workforce management.

Now, not every business function fits the formula. The functions must be supported by a large volume of data or be a function where a lot of manual auditing can be eliminated. But certainly functions like Marketing and Human Resources are a good fit for the WeDo model because you can audit those functions from both financial/assurance and performance goals.
WeDo hired experts at a consulting firms to get smart about the risks in various departments, then it designed controls for each department with the idea to offer continuous monitoring of processes.

**Customer Cultivation through User Events**

One other thing that distinguishes WeDo is the excellent way it leverages its annual User Conference.

Each year WeDo holds a user conference somewhere in Portugal. They rent a hotel in a beach resort or city (in 2015, Lisbon was the venue) and invite people from several dozen telecom customers to attend.

TRI attended the 2012 conference where they wined and dined their clients – and many educational sessions were given by customers. No public sales presentations are allowed, just the annual and refreshingly personal talk by Rui Paiva, WeDo’s CEO, who gives an update on WeDo, the company, plus the trends he’s seeing in telecom and the wider business assurance arena.

WeDo’s 2015 conference in Lisbon -- attended by 400 people from 150 corporations – highlighted the usefulness of RAID across telecom and other industries. Speakers hailed from Vodafone UK, 7-Eleven Mexico, PwC Brazil, Telecom Italia, Sonae Retail Portugal, and UPC Nederlands.

* * * * *

**About the Research Report**

*Telecom Fraud Management Services, Software & Strategies* is a 239-page market research report that analyses the struggles, challenges, successes, failures, and dreams of those who seek to control fraud in the telecom industry. The report’s emphasis is on solutions: the techniques, technologies, and tools that are working – and not working – to prevent or stop fraud. Authored by Dan Baker, TRI’s research director, the report draws on conversations with three dozen telecom fraud experts with major contributions by five top consultants in the field.

The report’s Executive Summary is freely available and the full report may be purchased by any telecom or fraud solution firm. In consideration for their financial support of this research, TRI has written vendor profiles on the fraud management activities of eleven solutions firms. In the body of the report, TRI discusses the activities of many other solution firms as well.

**About Technology Research Institute**

Technology Research Institute (TRI) has been writing and researching telecom software and systems markets since 1994. Its industry reports cover the gamut of telecom systems from billing and service assurance...to customer care and provisioning. In recent years, TRI has authored major reports on Revenue Assurance and Telecom Analytics & Big Data solutions. TRI also publishes two industry blogazines: *Black Swan Telecom Journal*, focused on revenue assurance, fraud, and analytics issues; and *Telexchange Journal*, which covers the wholesale, interconnect, and digital ecosystem partnering domain. TRI’s research director, Dan Baker, speaks at conferences such as *Capacity Magazine’s* Wholesale Fraud Forum and co-hosts podcasts on *Commsrisk*. 