

---

## **cVidya survey highlights concerns of revenue managers, fraud managers**

*Internal fraud is a growing concern, interconnect issues continue to cause revenue leakage, and convergent revenue and fraud solutions are being sought*

**Nov 16, 2010 10:10 PM,  
By Susana Schwartz**

After a busy couple of weeks with its Annual User Conference in Barcelona and then a Fraud Management Catalyst for Smart Phones demonstrated at Management World, I talked with vendor cVidya about the findings in its recent survey of 76 fraud and revenue assurance managers from 60 companies across 35 countries

To start, Cvidya found that the majority of respondents consider internal fraud a growing concern “because of more economic hardship in the global economy, the increasing value of personal information about people, and the availability of that information through internal systems,” explained cVidya’s Elias Chachak, vice president of marketing and business development. “With so many people in the chain--employees, sub-contractors, representatives, and dealers--operators’ fraud managers are having to redirect energies from outside the company in part to the inside of the company, where patterns of manipulations can possibly detected.”

Internal fraud generally falls into two categories: one type of which is to extract money out of the employer; the second focuses on exploiting data for a third-party interested in buying private information about customers.

Unfortunately, traditional fraud solutions generally do not focus on either of these types of internal fraud. For that reason, much of the process of finding and monitoring what is “under the radar” is done manually today. “For that reason, 85 percent of the respondents said they are concerned about these unmonitored fraud patterns,” said Chachak.

He believes telcos can learn a lot from banks and financial institutions, which monitor employees in real time to protect data—especially where exploitation can be disastrous to the customer and hence the company’s brand. “They are looking into solutions that do more sniffing into the network and look at which systems are accessed by which employees. If someone is going into the CRM system a lot or into a particular account too many times, a red flag goes up and a replay of activities can be conducted.”

This fact is making it particularly interesting in the area of point-of-sale in telecom, where mobile operators rely on dealers to do sales of phones. “This is particularly an area of concern in Eastern Europe,” noted Chackak, pointing out that 66 percent of respondents noted a conflict of interest exists when incentives and bonuses are based on activations and the

numbers of upgrades achieved. “They can fake activations of phone numbers or fake upgrades; in essence, creating ‘silent subscribers’ for a commission,” noted Chachak.

In terms of North America, Cvidya found that interconnect, or “bypass” fraud was a concern among 50 percent of respondents. “American carriers say they find more companies are trying to bypass settlement agreements by routing calls through other countries so that termination fees are lower,” Chachak said.

He also found that North American operators “lagged others” when it came to adoption of “standard risk assessment methodologies for revenue assurance,” such as those defined by TM Forum, which other operators in other countries focused on. “We found about 30 percent of operators internationally adopted standards, while only about 10 percent of American operators did,” he said.

In another part of the survey, North American companies were ahead, it seemed, in terms of convergent fraud and revenue assurance solutions for fraud managers and revenue assurance managers. “There is overlap in the collection of data—the same CDRs and phone calls to be processed, even though the risk management aspect is different with one focused on revenue assurance issues within an organization and the other focused on fraud outside of the organization,” Chachak said.

About 81 percent of respondents acknowledged fraud and revenue managers are sharing information for risk mitigation, but that manual processes make it more difficult. “This correlates to the increase in RFPs we see for converged solutions,” added Chachak. “In the survey, only 42 percent said they use tools that are integrated. They do recognize the value of automating the process; if revenue assurance managers find an employee deleted his brother’s account, that information also falls under the fraud manager’s purview.”