

---

## Insider Fraud: Detecting Criminal Activity in the Telecom Sales Process

Published by Dan Baker  
May 10th 2011

Telecoms spend an incredible amount of money on physical security to keep unauthorized eyes from seeing financial systems. They spend another big chunk of money on technical fraud systems and cybersecurity to prevent external fraudsters from stealing the family jewels.

Yet one of the biggest problems telecoms now face is fraud done inside their offices, dealer stores and firewalls by people fully authorized to transact business for the company. Welcome to the shady world of insider fraud, a growing area of operator concern according to fraud management vendor cVidya, who has just brought out a new version of its Fraud View solution to address the issue.

And here to tell us about it is Tal Eisner, cVidya's senior director, Product Strategy, and a guy who was once an investigator and manager at two leading mobile operators in Israel.

**Dan Baker: Tal, what's the genesis of insider fraud? And what's your evidence that it's becoming a bigger problem?**

**Tal Eisner:** Dan, as you can imagine, much of the data about fraud activity is closely guarded by the telcos. That's only natural. But what I will tell you is this: Our Fraud View product is installed at 130 telecoms in 63 countries and when a significant number of those customers raise a red flag around insider fraud, you can bet it's a big problem.

Another indicator that insider fraud is growing is common sense. Smartphones are expensive devices that are often subsidized by the carrier. Plus the smartphone will soon double as a mobile wallet. All these factors are going to make insider fraud easier to hide and more potentially damaging to an operator.

The forms of insider fraud vary greatly. Sometimes the fraud is perpetrated by an insider alone. In other cases, the insider helps someone outside commit fraud – sometimes deliberately, other times innocently.

The focal point of our investigation is all systems related to sales, the kind of systems that customer service reps, telemarketers and dealers have access to.

One of the drivers of insider fraud is all the pressure for wireless salespeople to meet aggressive revenue targets. And when people can't reach those targets, some will cook the numbers or artificially enhance the sales numbers by giving away services illegally – all to get their expected commission at the end of the month or quarter.

**DB: Are these things mostly happening within the enterprise accounts of telecoms?**

**TE:** No, it's not limited to enterprise sales alone. We're talking about the entire sales process becoming corrupted.

To give you an idea, one of the large U.S. mobile carriers told me the case of a door-to-door sales rep who committed fraud to the tune of millions of dollars. The salesman produced a great many deals of cell phones. Unfortunately, those deals were fraudulent: The customer actually never signed the agreements; their signatures were forged.

Much of the fraud happens because the fraudsters know how to navigate around the sales, prepaid, CRM or billing systems.

**DB: Is a lot of this happening because salespeople are getting their sales commissions upfront?**

**TE:** A few years ago, it's true, salespeople were getting sales commissions upfront and so there was a danger of signing up unqualified accounts. However, it doesn't work like that these days. Telecoms are more cautious about distributing commissions early these days.

**DB: What's the fraud management application look like here? Are you monitoring employee emails and Web searches?**

**TE:** Dan, I get this question all the time when I speak at conferences. No, our application has nothing to do with desktop applications that monitor emails or what sites users go to when they surf the Web.

We basically screen sales or money-oriented areas in IT, such as prepaid and customer-service systems. We are not recording all the activities being done by people. The purpose of our sniffing is to enable sales managers and fraud investigators to detect and see abnormal activities.

For example, it's normal for door-to-door salespeople selling iPhones and Blackberrys to immediately activate those phones as the sales happen. But if that same salesperson is activating three iPhones at 4 a.m., you might suspect something is wrong.

Another indicator of fraud is checks or credit card authorizations bouncing, typically a month or two months after the user is using the service, but after the dealer received his commission.

**DB: A couple years ago, I attended a conference session where Vodafone Germany gave a presentation on a dealer fraud/assurance system that employed a cVidya platform.**

**TE:** That particular system pre-dates the new insider fraud solution I'm talking to you about. The virtue of that system is that it detected how dealers were gaming the system in the way they juggled discounts or made offers in a way that maximized their commissions.

Some dealer- and in-house agents are far more daring in their fraud activities. Take the case of a dealer's agent who worked in one of the stores of a leading mobile company in Europe. He was a very bright salesperson. Unfortunately, he got himself into trouble by making some bad gambling bets, and he owed a lot of money to some bookies. He didn't have the money, so he cut a deal with the bookies, saying, "Come to my store every week or so, and I'll activate for free the most expensive handsets I have in the store. And each of these handsets will be deducted from my debt."

So that's exactly what happened. Somebody came to the store on a regular basis, went directly to him and "bought" handsets. And because the agent was very fluent on what needed to be done to activate customers, he went undetected for a long time. His strategy was not to open new accounts but to "glue" the illicit phones to existing corporate accounts, gambling that the corporations wouldn't take notice if a few phone accounts were added to their bill. But after a while, the enterprise customers were complaining about the extra charges, so he was eventually caught. If you had been regularly monitoring this guy's actions in the systems, you would have detected those kind of cases long before they got large enough to cause problems and jeopardize a key corporate account.

**DB: There are many cases where it would be hard to verify whether the dealer is doing right for the company. Take the examples of special discounts for students, senior citizens, etc.**

**TE:** Yes, in fact, it's a common practice to offer discounts to special demographic groups. But at the end of the month, if 20 iPhones were sold on a student discount, how many of them were actual students? To verify, you have to monitor ID cards and every other source of identification available. Likewise you need to monitor the salesperson's activities.

**DB: Nowadays, searching social-networking sites like Facebook might be another good place to find detailed information.**

**TE:** Actually in our latest version of Fraud View, we are integrating social networks as part of our investigation process – and we think we're the first fraud vendor to do that.

This is our philosophy: Get the investigator as much relevant information as possible. If it's Facebook, MySpace, Twitter fine. We've also integrated with Google Maps so if a subscriber gives you his home address and that address is in the middle of Central Park, you'll see that immediately. So in this way we're giving the fraud investigator the broadest view or angle on the case to decide whether or not this is fraud or not.

From my many years as a fraud investigator, I know that the most important challenge an investigator faces is deciding whether or not the case you have in front of you is fraud or nothing at all.

*Tal Eisner is senior director, Product Strategy, at cVidya. He has more than a decade of telecom fraud management experience. Prior to cVidya, Tal served as Fraud Management Department head at Orange Israel.*

*Dan Baker is the principal market synthesizer and co-founder of Technology Research Institute (TRI - <http://www.technology-research.com/>). He is also research director of a new online community, the Revenue Assurance Roundtable (<http://raround.com/>)*

(For the original article, please go to: <http://www.billingworld.com/blogs/baker/2011/05/insider-fraud-detecting-criminal-activity-in-the.aspx>)