# Subex Telecom Fraud Alerts

*March 2010*

**Internal fraud is on the rise**

Two separate incidents highlight the rise in internal fraud.

- Two large telecom operators in Italy were involved in a massive fraud, orchestrated by the Calabrian mafia. Arrest warrants have been issued to 56 people for their alleged involvement in the sale and purchase of non-existent international telephone traffic amounting to €2 billion ($2.7 billion) fraud and evasion of €400 million in VAT (Value Added Tax). The accused included CEO's of 2 large telecom operators of Italy. The fraudsters issued invoices for non-existent telecom services and siphoned large sums of money from the telecom operators. They achieved this by laundering the money abroad using companies and banks in locations such as Panama, Hong Kong, Luxembourg, Switzerland, San Marino, Vienna and London. The fraudsters also claimed VAT credits from the government.

  This incident is a testimony to the fact that internal fraud remains a huge threat and that no-one, however senior, is above suspicion.

**Source: SFGate, Feb 2010*

- Another case of internal fraud was detected in Zimbabwe, where a prominent telecom operator confirmed fraud of the value of US$1.7 million committed by its employees. The employees issued recharge cards and starter packs using manual invoices which were banned by the company. The operator discovered the fraud while modernizing and expanding its operations.

**Source: Zimbabwe Mail, Feb 2010*

**Mitigating internal fraud**

Internal fraud can be very different from external fraud. External fraud is usually impersonal, opportunistic and driven by pure greed. Internal fraud on the other hand may be driven by personal grudges or revenge. Internal fraud reveals the breakdown of internal structures, the relationship between employer and employee, and the lack of internal systems to provide safety nets, checks and balances. There are various ways to mitigate internal fraud, some of them are:

- Educate employees about policies and procedures, such as strict monitoring, penalization, whistle blower hotlines, etc
- Senior management should own the company's internal controls and keep a tight rein. Senior management's attitude is crucial for setting the tone from the top down
- Using automated systems to check misuse of critical functions
- Enabling deterrents by publicizing high profile fraud cases to deter would-be fraudsters from committing fraud in future

Internal fraud is a major threat and telecom operators need to take such steps to prevent and deter it.

**Major operator of Cramming busted by FTC**

Cramming is a practice that is still widespread and arguably under-regulated. In cramming, small charges are added to a consumer's bill without their consent. Fraudulent companies can add monthly charges to people's local phone bills thanks to Local Exchange Carrier (LEC) billing, and few phone users immediately notice the charges. If they do, it can be difficult to have them removed and obtain a refund.

Cramming became popular following the breakup of the telecom monopoly in US in 1980's. As part of the break up, phone companies continued to offer users a single bill that showed both local and long-distance charges, even though these came from different companies. This created the infrastructure for LEC billing: accepting charges from third parties and billing customers directly.

LEC billing was easy to abuse. Fraudsters would create a bogus company, convince the various LECs that they ran a legitimate operation, and then start sending them bills. Customers would pay, usually because they didn't check every charge on their bill each month. If the fees were kept low enough, they could continue for years before being discovered. The FTC has cracked-down on cramming through third-party verification, recording calls and keeping detailed records. In spite of these efforts, cramming is still prevalent, and in the US, the Federal Trade Commission (FTC) has recently obtained a court order against two brothers whose various enterprises pulled in $19 million over five years. This operator claimed that it used call centers in Philippines, India and Canada to cold call businesses. They would try to sell them $12.95-39.95/month products, all billed to the company's phone service rather than via a standard invoice. The real truth was that the vast majority of 'customers' never authorized any charges or bought any services. Even after the operator sent confirmation letters to its so called customers, a mere 0.25 percent responded to actually wanting the services. In fact,many respondents claimed they were billed fraudulently.

**Source: ARS Technica, Feb 2010*