

# Subex Telecom Fraud Alerts

December 2009



## CFCA releases Global Fraud Loss Survey 2009

The Communications Fraud Control Association (CFCA) has released the Global Fraud Loss Survey for the year 2009. The survey highlighted the following points:

- Estimated annual global fraud loss was **\$72-\$80 billion** in 2008 which is approximately **4.3%** of telecom revenues
- The estimated global fraud loss has **increased by 34%** from \$54-\$60 billion in 2005 to \$72-\$80 billion in 2008
- **91%** of respondents said global fraud losses had increased or remained the same
- Top 3 fraud types are
  - Subscription/Identity Theft: **\$22billion**
  - Compromised PBX/Voicemail systems: **\$15billion**
  - Premium Rate Service Fraud: **\$4.5billion**
- The top 5 hot spots (destination countries) for fraud are Cuba, Philippines, Liechtenstein, India and United Kingdom

For a copy of the complete report, please feel free to contact us.

*\*Source: CFCA fraud survey 2009*

## PBX fraud strikes Toronto, Canada

A small marketing firm in Toronto became a victim of toll fraud recently. The perpetrators gained access to the PBX system which allowed them to make calls to shell businesses overseas, earning them huge dollars in toll fees for every minute spent connected. After noticing an increase in the monthly bill of the firm (going from ~\$250/month to over \$4000) the operator contacted them to inform that their phone system might have been compromised. The operator suggested that the firm review existing network setup, and change all the voicemail passwords. The operator also blocked some of the toll numbers. But when the subsequent bill came in at more than \$63,000, it was clear the fraud hadn't stopped.

For more information on PBX hacking, please click on the link below  
[http://www.subexworld.com/pdf/PBX\\_%20Hacking.pdf](http://www.subexworld.com/pdf/PBX_%20Hacking.pdf)

*\*Source: thetelecomblog.com Dec 2009*

## Hot Fraud topics for 2010

The GSMA Fraud Forum is currently assessing which areas to focus efforts on in the coming year. Amongst the areas considered high on the priority list and in need of attention are:

- Roaming fraud prevention;
- Threats associated with new architectures and services;
- Prevention of revenue share fraud;
- Internet related fraud;
- Interconnect/Bypass/SIM-Box fraud.

## India blocks millions of mobile handsets for security reasons

On December 1, telecom authorities in India imposed a ban on all services to mobile phones without a valid identification number. The move will affect about 15 million cellular handsets, most of which are cheap imports from China.

The International Mobile Equipment Identity (IMEI) number is a 15-digit code which appears on the operator's network whenever a call is made. The absence of this number makes it impossible to trace either the caller or the phone or to access call details. Indian intelligence agencies say phones without the code have been used in attacks by militant groups. Mobile phones without the code were blocked at midnight - operators were asked to bar calls to them "in the wake of increased threat perception from militants".

*\*Source: BBC News, Economic Times, Dec 2009*