

Subex Telecom Fraud Alerts

November 2009



- **Subex supports International Fraud Awareness Week, November 8-14, 2009**

The International Fraud Awareness Week is a weeklong campaign established by the Association of Certified Fraud Examiners (ACFE), to encourage business leaders to proactively take steps to minimize the impact of fraud by promoting anti-fraud awareness and education. In keeping with our commitment to preventing and detecting fraud in the telecom industry, Subex is an Official Supporter of the Fraud Awareness Week. We would encourage our customers to also become Official Supporters by visiting the following link: <http://www.fraudweek.com/>

- **The New telephone 'scam' in Medway**

Fraudsters recently targeted a UK Operator's customers posing as their billing staff and informing them that a phone payment has not been made. The customers were informed that the phone would be disconnected if the payment wasn't made immediately. They also advised that there would be a significant charge for reconnection.

The fraudsters demanded the payment to be made by credit card right there and then.

To add credibility to their story they provided a 'demonstration' to customers that they could disconnect their phone line. This was achieved by taking advantage of the way the signaling works on the operator's network i.e. 'calling party clears'. So they actually just put the call on hold/mute and when the customer puts the phone down and tries to redial they have no dial tone. This may convince some customers that their line has actually been disconnected.

Other Telecom operators - particularly those using "calling party clears" technology - may wish to advise their customers of this threat.

- **EU Telecoms Reform enacts ePrivacy directive**

The European Parliament has released the revised ePrivacy Directive, following the agreement in early November on the EU Telecoms Reform. The revised ePrivacy Directive must be implemented by the Member States within 18 months. The new provisions will bring vital improvements in the protection of the privacy and personal data of all Europeans active in the online environment. The changes introduced include:

- for the first time in the EU, a framework for mandatory notification of personal data breaches . Any communications provider or Internet service provider (ISP) involved in individuals' personal data being compromised must inform them if the breach is likely to adversely affect them. Examples of such circumstances would include those where the loss could result in identity theft, fraud, humiliation or damage to reputation;
- reinforced protection against interception of users' communications through the use of - for example - spyware and cookies stored on a user's computer or other device;
- the possibility for any person negatively affected by spam , including ISPs, to bring effective legal proceedings against spammers;
- substantially strengthened enforcement powers for national data protection authorities. They will for example be able to order breaches of the law to stop immediately and will have improved means of cross-border cooperation.

- **Premium Rate Service Fraud Number Ranges**

The Australasian Telecommunications Fraud and Risk Association (ATFRA) have released a list of fraudulent numbers, which were identified by a telecom operator in APAC as part of their ongoing investigations on PRS fraud reduction. The concerned telecom operator has recommended that carriers bar these numbers at their International switch to avoid

losses. The operator has also released some PRS number ranges (not mentioned in this alert) which might be fraudulent. However, Subex would advise customers to be selective about barring such number ranges, because not only can it impact innocent businesses, but calls to many of the so-called fraudulent PRS ranges are being short-stopped anyway, so they're not even reaching the destined numbers.

Other global hotlist database resources are available to operators from industry associations such as GSMA and TRMA.

The fraudulent numbers released are as given below:

Antarctica 8823462275
Austria Mobile 43820944541
Avrasya 8819900033976
Bulgary 3598815406881
Cameroon 23722258929
CAR 236724937
Dominica 17675033767
Ellipso 881335184030
Emsat 88213213375
Estonia 3727022200
Georgia 2 99576000670
Globalstar TR 5922116475
Guinea Bissau 2452086569
Ivory Coast 22521709629
Liechtenstein 2 LOW 423662691870
Liechtenstein 2 LOW 423663900749
Lithuania 37091001960
Madagascar 261200203009
Madagascar 261229008309
Nauru 6744449290
Nauru 6745551330
Nauru 6749990310
Niger 227110020
Oration 88233790074
Sao Tome 239202137
Sao Tome 239210744
Sao Tome 239212231
Sao Tome 239294360
Sao Tome 239957460
Sao Tome 239982160
Sao Tome 239211347
Seychelles 248983280
Seychelles Mobile 248986002
Sierra Leone 2322227488
Sierra Leone 23222273950
Sierra Leone 23222285059
Somalia 25260993100
Somalia 25260951185
Togo 2285260309
UK Mobile 447537193959
Wallis & Fotune 681681052
Zaire 2437388060
Zaire 2434205099
Zimbabwe 263912794040

Follow the latest Fraud Management Trends on LinkedIn

http://www.linkedin.com/groups?gid=2285100&trk=myg_ugrp_ovr