

Mobile/Cellular Services Frauds in Africa

A Revenue Assurance White Paper

Each year Africa's mobile/cellular carriers lose the equivalent of almost one and three quarter *billion* US dollars through theft of service and related frauds. This study answers many of the questions pertaining to the levels of fraud and best practice Revenue Assurance (RA) approaches required to reduce that fraud in mobile cellular networks in sub-Saharan Africa. The author looks at the status and profile of the operators; how and with whom they are working to identify and rein in this epidemic of dishonesty and theft; and reduce revenue assurance marketing program errors. Current known types and techniques of fraud are also examined. Finally recommendations are made for the industry.

June 2012



www.4gafrica.org

Dedication

This research paper is dedicated to the robust African Telecommunications Industry.

Credits and Acknowledgements

The African Broadband Forum thanks and acknowledges World Stream Services and Subex for their able assistance in the research. A special thank you to Peter Scott-Wilson, a past director and CEO for many years at Market Research Africa MRA, for assisting in the hypotheses formulation and questionnaire design. The African Broadband Forum also thanks The Consultant Registry and Business and Technology Briefings, two US-based partners with global experience including Africa, for their assistance in the preparation of this report. Thanks to Sara Frewen the well known USA and SA based journalist for proof reading the paper in its various stages.

Copyright and Intellectual Property Notice

This document is copyright 2012 African Broadband Forum CC and is protected in all African countries and around the world by all applicable international copyright and intellectual property protection laws. No part of the material may be quoted, photocopied, reproduced or be stored by any electronic system without prior written permission.

Disclaimer

While every reasonable effort was taken to ensure the accuracy and soundness of the contents of this publication, neither the author nor the publisher will bear any responsibility for the consequences of any actions based on information contained.

Contact

William A. Hearmon, African Broadband Forum, bill@4gafrica.org

Mobile: +27829904443

Table of Contents

Executive Summary.....	1
Introduction	2
1.1 Terms of Reference.....	2
1.2 Research.....	3
1.2.1 Method and Data Employed.....	3
1.2.2 Definition of the Universe.....	3
1.2.3 Setting of Hypotheses.....	3
2.0 Findings	4
2.1 Respondent Profiles.....	4
2.2 Revenue Assurance Analysis.....	5
2.4 Operator Experience with Syndicate Detection and Eradication	6
3.0 Conclusions	7
4.0 Recommendations	7
Appendix A: Select Hypotheses	1
Appendix B: Letter of Appeal.....	1
Appendix C: Survey Results.....	2
Appendix D: About The Author.....	1
Appendix E: Glossary and Handy Website References	2
Handy Website References.....	3

Executive Summary

Network operators are embarrassed or barred from talking openly about their revenue assurance and fraud problems. In Africa the losses exceed 10% of revenue in many operations.

- Most fraud activity occurs around the pre-paid SIM card. The majority of African operators have more than 95% of their subscribers on pre-paid. Some at 99%.
- Bypass SIM boxes remain a major problem to locate and eliminate. This is more of a commercial and not a fraud issue.
- Most have RA losses of between 4% and 14% of revenue.
- Long Term Evolution tampers with the communications layers and will make it even easier for crooks to steal from the network cellular operator. "If you are not on top of revenue assurance yet be very careful when you introduce long term evolution (LTE)", said James Stewart of MACH in a recent webcast session.

Best Practice indicates that the winning operators have a holistic approach to fraud prevention and detection. There are definite opportunities for fraud and revenue assurance management (FRAM) integration suppliers in Africa. A dedicated African Association for Revenue Assurance would be well supported and a boon to help network operators quell this epidemic.

- Two-thirds of the African operators indicate that they would use a system integrator to implement their Fraud and Revenue Assurance Management (FRAM) processes. Half of those surveyed are firm on this. The remaining say that they would first want to be convinced of the value added by the FRAM Integrator. Further research is suggested to identify these specific network operators.
- Most operators (78%) would welcome the formation of an African Association for Revenue Assurance dedicated to assist them in RA matters. Possibly due to the staffing challenges which they highlight as prime.

A short selection of other researched outcomes from the study include:

- Subex Limited has the biggest share of RA system sales followed by cVidya.
- Ericsson remains the named major primary network supplier. Huawei and ZTE are ranked equally as being very close behind with network expansions.
- Thirty-three networks have budgeted to invest in Revenue Assurance systems this year. From the previous point on the use of a vendor partner offering a FRAM System Integrator Service one would surmise that the potential for this at two-thirds gives one a potential target market of twenty-two networks. PwC has the largest share of RA consulting services followed by E&Y and KPMG.
- Eighty-two per cent of respondents are first or second market leaders in their respective countries in terms of subscribers.
- More than half (57%) are partially satisfied that in-country syndicate operations have been stopped, while 28% say that this is not the case.

Introduction

In the field of Revenue Assurance (RA) with mobile cellular operations throughout Africa, stakeholders find that fraud and overzealous marketing campaigns are the largest contributors to losses. The techniques that management may bring to bear include hardware and software systems that profile users' behaviours and seek to detect and stop fraud timeously. Successful holistic approaches bring financial and auditing consultants and human relations and criminologists to the RA and risk management teams. Marketing campaigns to promote discounted buckets and bundles of airtime and VAS services need the wisdom of street-wise experts who understand the law of "unintended outcomes" before the launch creates large losses, and this is without cramping the style and enthusiasm of the innovative market dreamers.

1.1 Terms of Reference

With market research studies, one is attempting to ascribe a set of characteristics to a population group, or universe, by selecting and sampling a smaller portion of that group. Hypotheses are set and sampled via questioning techniques. The population for this study into Revenue Assurance were all the mobile cellular operators in sub-Saharan Africa. There are seventy-eight GSM and eleven CDMA operators active in the region. Forty-eight of these operators were sent questionnaires. Eleven responded.

One immediate challenge highlighted by this research study is the one of confidentiality and embarrassment. Asking mobile RA operations management questions about loss and fraud is tantamount to asking a family about alcoholism or drug addiction. Most mobile networks are at the forefront of PR awareness in the public domain. Half of the operating networks are controlled by three public listed multinational conglomerates. These are MTN, Airtel (Bharti) and Vodacom/Vodafone. Their managers will tend to clam up when answering questions on these sensitive subjects. Yet the research had to be done and the answers found to slow this RA loss pandemic down to a blur. The response rate of 23% over three months is indicative of this factor. Others reasons include the availability of correct departments and names of risk and RA managers in the companies surveyed. The GSMA list which is primarily the roaming manager in each operation was used to contact the current GSM operators. The author's own database of GSM and CDMA operations staff created over six years, was included. In the letter of appeal each recipient was asked to forward the letter and questionnaire to the responsible risk or RA manager to complete.

1.2 Research

Raw, actionable knowledge is the key to any successful effort. This section describes how the research for this paper was conducted.

1.2.1 Method and Data Employed

There are 55 countries on the African continent with 48 in sub-Saharan Africa. Surveying by email is the most optimal method and advisable to collect the data quickly. The down side is that there is so much spam and viral communication received hourly by respondents that one is at risk of being ignored or blacklisted. To overcome this challenge a few different ISP's and email addresses were used a number of times. The Mail Chimp email service was utilised.

Pretesting: A questionnaire with 20 questions was developed with the aid of WSS, Subex in India and Peter Scott-Wilson a long time market research fellow. Subex is a large supplier of systems to prevent and detect revenue assurance mistakes and fraud, amongst others. WSS is a FRAM systems integrator based in Mauritius. This one-page questionnaire was designed and tested locally and in person with the head of risk management at Vodacom and the RA team at MTN.

The questionnaire and letter of appeal were designed with:

1. A letter of request for co-operation with confidentially affirmed
2. Explanations of terms
3. Sought data
4. Classification data
5. Identification data (limited)

The questionnaire and accompanying letter of appeal are in the Appendix.

1.2.2 Definition of the Universe

The population, or universe, consists of all mobile communications operators in sub-Saharan Africa. Names and addresses collected over the past few years and the GSMA contact list was used. A drawback of the GSMA list is that the majority listed are roaming contact managers. Although the addressees were asked to pass the survey questionnaire on to the responsible RA or risk manager there was no guarantee that this would happen.

1.2.3 Setting of Hypotheses

Hypotheses are tentative solutions set up for test. Each hypothesis must be accepted, rejected or modified according to the preponderance of the best available evidence. The list of draft hypotheses selected is in the Appendix. They are not in order and not all were tested exactly as listed.

2.0 Findings

In the Appendix is a copy of the results from the survey. As eleven questionnaires were returned, the response rate was 23%. This is acceptable compared with similar types of surveys which normally yield a 10% to 20% response rate.

2.1 Respondent Profiles

The Respondent Profiles are covered in Questions 1 to 10.

Eleven GSM operators responded from ten different countries. In addition to GSM systems, two run fixed WILL services; one CDMA and four WiMAX or WiFi. Two have more than three million subscribers; three between 1 and 3 million; and one between 100,000 and 500,000 subscribers. The other five did not respond to this question.

Five are the market leaders in their country; four are second and two, third.

Forty-eight networks have less than 5% *postpaid subscribers*. Most fraud activity occurs with the prepaid SIM card. This is a major reason why many African operators have high fraud rates of 13% compared with USA and Europe who are mostly postpaid and have fraud below 1,5%.

Healthy growth rates are expected. Twenty-one operators of the total population in Africa are expecting subscriber growth of more than 20% in the next year; another 21 between 10% and 20%; 21 between 5% and 10% and 14 with less than 5%.

The major *network vendor* remains Ericsson with 73% share. Eight respondents name them as their supplier. This agrees with the known market of 48 networks out of 78 in sub-Saharan Africa. There is an overlap now as many networks are procuring their expansions from Huawei and ZTE. Survey results show six each. One gave Alcatel and none to Nokia Siemens Networks NSN. The two largest operators in Africa with multiple country properties are MTN with 18 in (sub-Saharan Africa)and Airtel with 16 networks. Both use and have used Ericsson as their prime core supplier. We do know that originally there were 17 with Alcatel as core network supplier and NSN with ten. The situation is clouded with Huawei and ZTE making very good inroads for many reasons including low prices, long payment terms and attractive vendor financing packages. This is countered by complaints of training shortcomings, equipment quality, delivery delays and contract renegotiations during systems delivery, installation and commissioning. Should base station deployments be the prime market share criterion then the two most prolific countries in Africa would be Nigeria and South Africa. They have over 40,000 BTS installed. NSN would then have a larger share than purely on a per country system sales basis.

Half of the African networks have installed data services for their subscribers using a combination of GPRS with EDGE, UMTS and WiFi or WiMAX. UMTS (read WCDMA and HSPA) is in 25 networks. With WiFi and WiMAX also in 25. It is not certain if these are the same networks with overlaps.

The bulk of the respondents (45%) were in a Revenue Assurance department (under finance). Twenty percent each were either in the finance or technical divisions. The question was possibly ambiguous to some.

2.2 Revenue Assurance Analysis

Questions 11 to 24 cover the Revenue Assurance Analysis.

The Finance Department controls 55% and the CEO 36% of Revenue Assurance activities, with 9% not responding to the question. Their multiple activities included 39% fraud; 22% collections; 22% Interconnect payments and 17% top up sales.

Their benchmarking is 42% to Industry Standards, 24% to International Standards, with 17% each to In-Country and Your-Group standards.

Estimated annual losses with 43% of the respondents cite between 4% and 14% of revenue missing. Another 43% indicate that it is between 2% and 4% of revenue. The last 14% cite less than 2%. No comment was received from 36% of respondents.

Asked if there had been an increase in fraud and RA losses over last year, 77% indicated that fraud and RA losses had reduced, 22% increased. No comment was received from 36% of respondents.

Budgeted Fraud RA management systems investment for next year: 22% will spend more than \$1 million, 11% between \$200K and \$750K, 11% less than \$220K and 55% say zero spend. It would be worth another investigation for suppliers to find these 33 suppliers who want to buy RA systems.

External agency settlement accuracy confidence is: 63% acceptable, 25% lack confidence, 12% having no problems.

Interconnect Revenue from both local and international sources is 56% with less than 20% of revenue, 22% between 20% and 40% revenue, 11% between 40% and 60% ,and 11% with more than 60% revenues from Interconnect. The abuse of SIM Boxes affect this bypass. The well known industry consultant and colleague of the author, Robert Pasley states, "I would not say a SIM box caused no loss. However, I would not class a SIM box as "fraud" as it legitimately uses a paying service on the network – regardless if it is "less profitable" for the operator. It is really up to the operators to ensure that no arbitrage exists that can be exploited in this manner – which, in my view, is a commercial issue rather than a fraud issue". Wise words.

Regarding the biggest challenge in running RA systems the survey shows difficulties in four areas with the following weighting: People and Staffing 38%, Network Issues 24%, Domain Skills 19% and Funding 19%.

When ranking their respective return on investment (ROI) on the RA system they indicated: Acceptable 50%, Excellent 25% and Improving 25%.

The external consultancy services most used for RA were: PwC 56%, E & Y 38%, KPMG 11% and Deloitte had none.

The suppliers of RA management systems were: Subex 50%, cVidya 33%, MDA 17% and none for WeDo. Two-thirds of the respondents would use a system integrator (SI) to implement a FRAM system. Half of these are resolute. The other half would first like to ascertain the value added from the system integrator. Further research is suggested with African networks to identify these specific twenty-five operators who would like to use the systems integration services.

2.2 Fraud Techniques

Question 25 lists 19 known fraud methods. See questionnaire list in Appendix.

When it comes to the types of fraud perpetrated the largest problem remains the use of Bypass SIM Boxes. Ranked first in previous studies, confirmed by MTN, in this study it ranks with 20% of operators suspecting their use in their networks. A Bypass SIM Box bypasses the interconnect and the fee arising by using an IP connection whereupon the overseas operator receives no payment.

Next of importance is 10% prepaid fraud, with internal staff fraud and subscription fraud at 5% each. The other fraud perpetration methods ranked mostly the same with all operators. These are SIM cloning, call selling combined with subscription fraud, International Revenue Share Fraud (IRSF) to premium numbers, box splitting, shoulder surfing, bill spreading, SIM stuffing, bulk SMS and MMS spam, voicemail frauds, ISP fraud, QOS manipulation (it is confirmed that this will be bigger with LTE), tolls and rules tampering, data fraud, dealer fraud and others (many to be developed and discovered).

These results need to be researched and further verified by companies interested in refining the details to the levels of fraud using each technique.

2.4 Operator Experience with Syndicate Detection and Eradication

Questions 26 to 30 query operator experience with syndicate detection and eradication.

The level of confidence that fraud from syndicates has been stopped is 57% at a medium level, 28% at a low level and 14% just do not know.

Forty-four percent indicate that no syndicates have been detected in their country, 22% have had more than five syndicates caught, and 11% have had between one and four syndicates found.

In their own companies 56% have found no syndicates working to steal, 22% found between one and four syndicates, 22% more than five syndicates and 25% do not know.

Satisfaction with the RA system provider is at 50% fair, 38% good and 13% were delighted.

The final survey question asked if they would actively support the formation of an African Association for Revenue Assurance. The bulk of 78% indicated yes, 11% no and 11% perhaps.

3.0 Conclusions

Numerous inferences are possible based on the data made available in this report and interpreted in the light of experiences and views of the reader. The following are some of the most compelling conclusions drawn by the author.

- There is a definite advantage for network operators to benefit from the "holistic" approach to fraud and RA mistake prevention and early detection.
- There is a real need and perceived demand to market and sell FRAM integration services to mobile cellular network operators in Africa. An obvious conclusion from the "Depends on Value" question and response is that the integrator company creates a brilliant value added offering to bring to the market. Target this to the 45 networks yet to be identified.
- In-country syndicates have been apprehended in the main.
- An African association dedicated to revenue assurance would be welcomed and supported.

4.0 Recommendations

More detailed research needs to be conducted on the fraud methods prevalent in African networks today with a system of immediate dissemination of new fraud techniques as they are discovered.

Like-minded network operators, management consultants, system suppliers, audit companies, human relations specialists and sociologists (criminologists) need to be gathered together in order to bring this holistic approach to reducing the wholesale theft, which is at epidemic proportions in Africa. With the internet protocol all IP based long term evolution LTE on the horizon this situation will worsen tenfold.

A vibrant and active African Association of Revenue Assurance AARA dedicated to this end and unique for African networks would be one complimentary vehicle. The AARA would run a confidential web based discussion forum for operator only members to exchange ideas and expose new methods recently encountered and blocked in their networks. Syndicates will hate this. White papers would be published in the association website. Frequent conferences would be held in the region at practical collegiate levels as opposed to vendor driven. The specialists listed in the above paragraph would take part in panels, workshops and discussion groups. The existing RA associations, training and accreditation agencies would be invited to participate as fellow members of the AARA.

Appendix A: Select Hypotheses

Some hypotheses selected were:

1. Ascertain to what extent an operator's audit services company are involved in Revenue Assurance and the prevention of fraud. Are most frauds caught retro actively?
2. Which of the big four accounting firms are predominant in Africa in the telecommunications industry?
3. Who are the leaders in Revenue Assurance? Two questions.
4. Cellular operators in Africa with less than 4 million subscribers will enthusiastically contract an integrator company (associated with another non-competing operator) with experience in installing and integrating a new RA and fraud system into their operation.
5. Estimate what value they would place on this service.
6. Test loss perception in Africa in comparison with the worldwide Subex research which indicated that there is a considerable and important gap between Acceptable losses, Estimated losses and Actual losses. Subex's 2007 survey results were acceptable = 1,8 %, with estimated = 3,6 % and actual = 13,6%. We feel it may be worse in Africa thus giving more impetus to companies selling integration services.
7. Estimate the level of awareness in migration fraud in these operators in Africa.
8. Estimate the awareness level of bypass SIM box interconnect fraud in these networks. Barring internal fraud bypass SIM box fraud is the single biggest source of revenue leakage. Test this via the MR questionnaire.
9. Analyse and test via questions a comprehensive range of types of fraud listed below:
 - i) Subscription fraud viz. false or stolen data used by subscriber
 - ii) Cloning, two SIM cards but only one is charged
 - iii) Call selling; combines with subscription fraud
 - iv) PRS revenue inflation; creates a fake PRS number through subscription fraud but the operator still has to pay the VAS. See Glossary of Terms.
 - v) Box splitting and migration; sold in bundles to speed up penetration then remove SIM and sell mobile equipment in another country or area
 - vi) Shoulder surfing, records numbers and pins for self use or to sell for flat fee
 - vii) Bill spreading: small amounts on fraudulently acquired accounts not highlighted heuristically by system and not investigated but bills remain unpaid with considerable losses
 - viii) GSM SIM Stuffing: using multiple stolen SIMS on same equipment
 - ix) SMS DOS abuse: large volumes of SMS to one subscriber "loading" them with texts. Goes to many subscribers too
 - x) Voicemail frauds

Subex assisted by sending their relative Rankings of these known Fraud techniques for inclusion in question 25.

Appendix B: Letter of Appeal



January 2012

African Broadband Forum research project into Revenue Assurance in Africa.

At the African Broadband forum we are studying the needs of companies for Revenue Assurance systems. I'd be grateful if you would answer a few questions to help us. It won't take more than a few minutes of your time. Your replies will be regarded as strictly confidential and will be used solely for a research project to help the industry in Africa.

The aim of the report is to aid system designers, audit companies and vendors in satisfying your demands for Revenue Assurance solutions. The results will not be used for commercial gain by any company or group of companies nor me. The RA vendors, auditors and consultants will receive identical copies of the findings and recommendations. Please try to answer all the questions wherever possible as this will make the research more valuable. We ask you to forward this to the right person.

Thank you very much, in advance, for your assistance.

Bill Hearmon

A handwritten signature in black ink, appearing to read 'Bill Hearmon'.

Chairman African Broadband Forum

Appendix C: Survey Results

Appendix D: About The Author

William (Bill) Hearmon

African Networking, Telecommunications and Security Consultant
bill@4gafrica.org



Born in Johannesburg, **William (Bill) Hearmon** is the Chairman of the African Broadband Forum.....a trade association for operators in Africa. Bill has a BSc in Electrical Engineering from the University of the Witwatersrand, where he specialised in microwave systems and the stability of power systems. He then went on to a five-year stint for Siemens in Johannesburg and Munich, and then to Motorola for fifteen years reaching the position of Director of Sales for Africa in Cellular Networks. Bill is an MBA graduate from the University of Cape Town, a Fellow of the SA Institute of Electrical Engineers and was the CEO and Founder of a number of companies based in Botswana and South Africa. His specialist consulting interests are Marketing Research, Industry Expert Witness, Private Investigations into Fraud and Revenue Assurance, Sales and Business Development and Acquisitions Discovery and Analyses.

Appendix E: Glossary and Handy Website References

Glossary

RA	Revenue Assurance
AARA	African Association of Revenue Assurance
FRAM	Fraud and Revenue Assurance Management
IRSF	International Revenue Share Fraud
SIM	Subscriber Identity Module
SIM boxes	A GSM gateway, two phones on different networks, rigged so that a call arriving on one is routed out again on the other.
SIM cloning	Duplicating the GSM motor (each GSM mobile phone contains a GSM motor) identification and placing calls/SMS/data services using the account of a cloned GSM motor
Shoulder surfing	A security attack where the attacker uses observation techniques, such as looking over someone's shoulder to get information
SIM stuffing	"stuffing" of the SIM with illegal recharges either through manipulation of network elements or with HRNs. It is different from SIM cloning in that it uses
CDMA	Code Division Multiple Access
GSM	Global System for Mobile Communication
GSMA	GSM Association for mobile operators
GPRS	General Packet Radio Service
EDGE	Enhanced Data Rates for Global Evolution
HSPA	High Speed Packet Access
LTE	Long Term Evolution. Wireless broadband technology designed to support Internet access via cell phones and handheld devices
QOS	Quality of Service
VAS	Value added service
WILL	Wireless in Local Loop

WCDMA	Wideband Code Division Multiple Access
NSN	Siemens Network
MACH	Leading provider of hub-based mobile communications
E&Y	Ernst and Young
PwC	Price Waterhouse Cooper
PRS	Premium Rate Service
SI services	System Integration services

Additional information on telecom terminology can be obtained from:

<http://www.carrieraccessbilling.com/telecommunications-glossary-a.asp>

Handy Website References

Telecommunications UK Fraud Forum

<http://www.tuff.co.uk/home.asp>

IQPC Conferences on Fraud Events

<http://www.telecomsfraud.com>

The Global Revenue Assurance Professional Association (GRAPA)

<http://www.grapatel.com/default.asp>

TM Forum

<http://www.tmforum.org/AbouttheTMForum/730/home.html>