**Islamic University of Gaza**
**Deanery of Graduate Studies**
**Faculty of Commerce**
**Department of Business Administration**

# Detecting Fraud in Cellular Telephone Networks

## "JAWWAL" Case Study

**By**

**Hiyam Ali El Tawashi**

**Supervised By**

**Prof. Yousef Hussein Ashour**

“A Thesis Presented in Partial Fulfillment of the Requirement for the Degree in "MBA"

**August, 2010**

بسم الله الرحمن الرحيم

(وَإِن يُرِيدُواْ أَن يَخْدَعُوكَ فَإِنَّ حَسْبَكَ اللّهُ هُوَ
الَّذِيَ أَيَّدَكَ بِنَصْرِهِ وَبِالْمُؤْمِنِينَ)

[الأنفال: 62]

# Detecting Fraud in Cellular Telephone Networks
# "JAWWAL" Case Study

## ABSTRACT

Telecommunication fraud is a problem that has grown dramatically over the past ten years. Fraud become a serious global issue for mobile network service providers, it has undoubtedly become a significant source of revenue losses and bad debts to telecommunication industry, and with the expected continuing growth in revenue it can be expected that fraud will increase proportionally.

The research project therefore, focused on how Jawwal Company managing and detecting the fraud, in order to modify the current tools for more effective fraud prevention and detection, for this reason the researcher undertook a set of actions that are reported as follow:

First step it was necessary to understand the problem of telecom fraud, then to know what makes people perpetrate the fraud, and which are the most prevalent fraud types that are occurring, clarifying which is the likely products and services to be attacked, what source of information to facilitate the fraud, how fraudsters perpetrate the fraud finally explaining the fraud detection and prevention procedures.

Then apply the study on Jawwal Company as study case, by distributing 200 questionnaires to targeted sections, and analyzing the result which shows that the current fraud management at Jawwal Company is not efficient and needs to be modified.

# منع التحايل في شبكات الهواتف الخلوية

# دراسة حالة (شركة جوال)

## Arabic abstract

تفاقمت مشكلة التحايل على شبكات الاتصالات خلال العشرة سنوات الماضية، ولهذا هنالك اهتمام عالمي بموضوع منع التحايل، ولا شك أنه كلما زادت الرغبة في تحقيق المزيد من الأرباح سيقابل ذلك بزيادة مخاطر التحايل.

في هذا البحث، ناقش الباحث كيفية إدارة مشكلة التحايل من قبل شركة الاتصالات الخلوية الفلسطينية جوال. وذلك بهدف تقويم الطرق والأساليب الحالية من أجل فعالية أكثر في التعامل مع مشكلة التحايل.

بداية قام الباحث بالإحاطة بجميع جوانب مشكلة التحايل، من خلال تعريف مشكلة التحايل وفهم دوافع المشتركين للقيام بها، ومن ثم توضيح أنواع التحايل وما هي أكثر الخدمات والمنتجات عرضة للتحايل وما هي قنوات المعلومات التي تسهل ارتكاب التحايل، وفي النهاية استوضح الباحث كيف تتم الوقاية والمنع للتحايل، ولقد استخدم الباحث المنهج الوصفي التحليلي.

قام الباحث بالدراسة الميدانية من خلال توزيع 200 استبان على أفراد العينة، ثم بتحليل النتائج التي كان أهمها أن وسائل وأساليب منع التحايل في شركة الاتصالات الخلوية جوال غير فعالة وبحاجة إلى تقويم لتصبح أكثر فعالية.

# ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my supervisor **Prof. Dr. Yousif Ashour**, for his valuable guidance and advice. He has been very supportive and patient throughout the progress of my thesis.

## DEDICATES

**I dedicate this work to:**

- My parents'…
- My son…
- My colleagues at Jawwal Company…

# LIST OF ACRONYMS

| | |
|---|---|
| 3G | Third Generation |
| AUC | Authentication Center |
| CDR | Call Detail Record |
| CFCA | Communications Fraud Control Association |
| DAM | Direct Access Method |
| DISA | Defense Information Security Agency Direct Inward System Access |
| DTMF | Dual Tone Multi Frequency |
| EL | External Linkages |
| ETSI | European Telecommunications Standards Institute |
| FIINA | Forum for International Irregular Network Access |
| FMS | Fraud Management System |
| GPRS | General Packet Radio Service |
| GSM | Global System for Mobile Communications |
| HLR | Home Location Register |
| HRN | Hidden Recharge Number |
| HUR | High Usage Report |
| ID | Identity Document |
| IDA | Indirect Access |
| IDD | International Direct Dealing |
| IMEI | International Mobile Equipment Identity |
| IMSl | International Mobile Subscriber Identity |
| IP | Internet Protocol |
| IRS | Internal Revenue Service |
| ITU | International Telecommunication Union |
| KI | Individual Subscriber Authentication Key |
| KPls | Key Performance Indicators |
| LAN | Local Area Network |
| MSISDN | Mobile Subscriber ISDN number |
| NRTRDE | Near Real Time Roaming Data Exchange |
| OPCOs | Operating Countries |

| | |
|---|---|
| PBX | Private Branch Exchange |
| PDA | Personal Digital Assistant |
| PIN | Personal Identification Number |
| PLMN | Public Land Mobile Network |
| PRS | Premium Rate Service |
| PTT | Postal Telephone and Telegraph |
| SDR | Service Difficulty Reports |
| SIM | Subscriber Identity Module |
| SLU | Single Line Unit |
| SMS | Short Message Service |
| TAP | Test Access Path |
| TUFF | Telecommunications UK Fraud Forum |
| VAS | Value Added Services |
| VolP | Voice Over Internet Protocol |
| VPN | Virtual private Network |
| WAN | Wide Area Network |
| WAP | Wireless Application Protocol |

# TABLE OF CONTENTS

**Abstract** ........................................ **IV**
**Arabic abstract** ........................................ **V**
**Acknowledgement** ........................................ **VI**
**List of acronyms** ........................................ **VIII**
**Table of contents** ........................................ **X**
**List of tables** ........................................ **XV**
**List of figures** ........................................ **XIX**

**CHAPTER [1]: INTRODUCTION** ........................................ **1**

1. 1 Background to the Study ........................................ **2**
1. 2 Difficulties in Detecting Fraud ........................................ **2**
1. 3 Definitions of Terms to be used in the Research ........................................ **4**
1. 3. 1 Telecommunication Fraud ........................................ 4
1. 3. 2 Bad Debts ........................................ 4
1. 3. 3 Revenue Assurances ........................................ 4
1. 3. 4 Fraud Prevention ........................................ 4
1. 3. 5 Fraud Detection ........................................ 4
1. 4 Statement of the Problem ........................................ **5**
1. 5 Research Variables ........................................ **5**
1. 6 Objectives of the Study ........................................ **5**
1. 7 Importance of the study ........................................ **6**
1. 8 limitations of the study ........................................ **6**
1.9 Research Design ........................................ **7**

**CHAPTER [2]: LITERATURE REVIEW** ........................................ **9**

**SECTION 1: TELECOM FRAUD OVERVIEW** ........................................ **10**
2. 1. 1 What is Telecom Fraud? ........................................ 11
2. 1. 2 Some Recent Figure about Telecom Fraud ........................................ 11
2. 1. 3 Some Factors Leading to Telecom Fraud ........................................ 12
2. 1. 4 Where Doe's Fraud Exists? ........................................ 12
2. 1. 5 Does Fraud Differ by Geography? ........................................ 12
2. 1. 6 How Much Damage is Fraud Doing? ........................................ 13
2. 1. 7 What is The Real Cost of Fraud? ........................................ 13
2. 1. 8 Fraud Positioning Approaches ........................................ 14
2. 1. 9 Fraud Management Approaches ........................................ 15
2. 1. 9. 1 FM Approach 1 ........................................ 15
2. 1. 9. 2 FM Approach 2 ........................................ 16
2. 1. 9 . 3 FM Approaches 3 ........................................ 16
2. 1. 9. 4 FM Approach 4 ........................................ 16
2. 1. 10 What's the Difference Between a Fraud and a Bad Debt? ........................................ 17
2. 1. 10. 1 Effects and Impact of Bad Debt ........................................ 17
2. 1. 10. 2 Effects and Impact of Fraud ........................................ 17
**SECTION 2: WHAT MAKES PEOPLE PREPERATE THE FRAUD** ........................................ **19**
2. 2. 1 Who Actually Commits Fraud? ........................................ 20
2. 2. 2 Where Do Fraudsters Work From? ........................................ 20
2. 2. 3 Why Do Fraudsters Do It? ........................................ 20

2. 2. 4 Some Motivation for Committing the Fraud ... 21
2. 2. 4. 1 Financial Gain ... 21
2. 2. 4. 2 Revenue Fraud ... 21
2. 2. 4. 3 Anonymity ... 22
2. 2. 4. 4 Lack of legislation and prosecution ... 22
**SECTION 3: WHICH ARE THE MOST PREVELANT FRAUD TYPES THAT ARE OCCURING ... 24**
2. 3. 1 Subscription Fraud ... 25
2. 3. 2 Usage/ Airtime Fraud ... 25
2. 3. 3 Unauthorized Service Fraud ... 25
2. 3. 4 Sales and Dealer Fraud ... 25
2. 3. 5 Technical Fraud ... 26
2. 3. 6 Internal Fraud ... 26
2. 3. 7 Equipment Fraud ... 27
**ECTION 4: WHICH ARE THE LIKELY PRODUCTS AND SERVICES TO BE ATTAKED? ... 28**
2. 4. 1 The Fraudsters Attacked the Weakest Link in the Operator ... 29
2. 4. 2 What Does Get Targeted? ... 29
2. 4. 2. 1 Fixed Lines ... 29
2. 4. 2. 2 Indirect Access (IDA) ... 29
2. 4. 2. 3 Mobile ... 30
2. 4. 2. 4 VOIP services ... 30
2. 4. 2. 5 Postpaid Service ... 30
2. 4. 2. 6 Prepaid Service ... 30
2. 4. 2. 7 Satellite ... 31
2. 4. 2. 8 Value Added Features and Services (VAS) ... 31
2. 4. 2. 9 Roaming Service ... 32
2. 4. 2. 10 Premium Rate Services (PRS) ... 32
2. 4. 2. 11 Customer Confidential Information ... 33
2. 4. 2. 12 Selling of Information ... 33
2. 4. 2. 13 E- Commerce Services ... 33
2. 4. 2. 14 M - Commerce Services ... 34
2. 4. 2. 15 Webcare Systems ... 34
2. 4. 2. 16 Warehouses, Dealers, Sales Outlets ... 34
2. 4. 2. 17 Calling Card ... 34
2. 4. 2. 18 Payphone ... 35
2. 4. 2. 19 Private Branch Exchange (PBX) ... 35
**SECTION 5: WHAT IS THE SOURCE OF INFORMATION TO FACILITATE THE FRAUD? ... 36**
2. 5. 1 Information is Power ... 37
2. 5. 2 Sources of Information ... 38
2. 5. 3 Employee Compromise ... 38
2. 5. 4 Sale Channels ... 38
2. 5. 5 Vendors ... 39
2. 5. 6 Media ... 39
2. 5. 7 Internet ... 39
2. 5. 8 New Generations of Networks ... 40
2. 5. 9 Customers ... 40
2. 5. 10 Suppliers ... 40

2. 5. 11 Competitors........................................................................................ 40
2. 5. 12 Fraud Information Sharing.......................................................................... 41
**SECTION 6: HOW IS FRAUDESTERS PREPERATING THE FRAUD?............ 42**
2. 6. 1 Leading GSM Fraud Risks ......................................................................... 43
2. 6. 2 Things Fraudsters Want to Know ................................................................ 43
2. 6. 3 Three Main Fraud Driven Types ................................................................. 44
2. 6. 4 People Driven fraud ................................................................................... 44
2. 6. 4. 1 Social Engineering..................................................................... 44
2. 6. 4. 2 Pre Texting ................................................................................ 45
2. 6. 4. 3 Dealer Fraud .............................................................................. 45
2. 6. 4. 4 Identity Theft ............................................................................. 46
2. 6. 4. 5 Subscription Fraud..................................................................... 46
2. 6. 4. 6 Controlling the Risk of Subscription Fraud.................................... 46
2. 6. 4. 7 Extending the Fraud – Paper Company/Long Firm Fraud ................ 47
2. 6. 4. 8 Extending the Fraud – Bill Spreading ............................................ 47
2. 6. 4. 9 Extending the Fraud – Address Changing...................................... 48
2. 6. 4. 10 Payment Fraud Types ................................................................ 48
2. 6. 4. 11 Providing Tools and Information fraud ........................................ 49
2. 6. 4. 12 Unauthorized Bonuses or Account Credits fraud (internal fraud).... 50
2. 6. 4. 13 Physical Security Compromise Fraud .......................................... 50
2. 6. 5 Product/Process Driven................................................................................ 50
2. 6. 5. 1 Call Features Abuse.................................................................... 50
2. 6. 5. 2 Call Forward Fraud..................................................................... 51
2. 6. 5. 3 Conference Calling Fraud............................................................. 51
2. 6. 5. 4 GSM Call Selling ....................................................................... 51
2. 6. 5. 5 Roaming Fraud .......................................................................... 52
2. 6. 5. 5. 1 Cost of Roaming Fraud ............................................................. 52
2. 6. 5. 6 GSM Cloning.............................................................................. 53
2. 6. 5. 7 Bypass........................................................................................ 54
2. 6. 5. 8 SIM Boxes .................................................................................. 54
2. 6. 5. 9 Interconnect Re-origination........................................................... 54
2. 6. 5. 10 Prepaid Fraud............................................................................ 54
2. 6. 5. 10. 1 Prepaid Fraud Attacks ............................................................ 55
2. 6. 5. 11 Top Up Fraud – 3rd Party Compromise ........................................ 55
2. 6. 5. 12 GPRS Overbilling...................................................................... 55
2. 6. 5. 13 Calling Card Fraud .................................................................... 56
2. 6. 5. 14 Shoulder Surfing....................................................................... 56
2. 6. 6 Technology Driven Fraud ............................................................................ 56
2. 6. 6. 1 SS7 Manipulation Fraud.............................................................. 56
2. 6. 6. 2 Blue jacking Fraud...................................................................... 56
2. 6. 6. 3 Bluesnarfing Fraud ..................................................................... 57
2. 6. 6. 4 DISA/PBX Fraud........................................................................ 57
2. 6. 6. 5 VOIP Risks ................................................................................ 57
2. 6. 6. 6 IMEI Duplication......................................................................... 58
2. 6. 6. 7 Phone Theft ............................................................................... 58
2. 6. 6. 8 SMS Inflation ............................................................................. 58
2. 6. 6. 9 Mailbox/Voicemail Fraud............................................................. 59
2. 6. 6. 10 Ghosting .................................................................................. 59
2. 6. 6. 11 Box Splitting............................................................................. 59

**SECTION 7: DETECTION AND PREVENTION ...................................................... 60**
2. 7. 1 Basic Principles and Requirements........................................................ 61
2 .7. 2 Recommendations about Where Loopholes Exist and How they Should be Minimized or Closed ........................................................................ 62
2. 7. 2 .1 Fraud vs. Bad Debt (Receivables) Separation.................................. 62
2. 7. 2. 2 Call Detail Analysis.......................................................................... 63
2. 7. 2. 3 Roaming Fraud Management ........................................................... 64
2. 7. 2. 4 Applying Roaming Restrictions ....................................................... 64
2. 7. 3 Prevention and Detection – Prepaid Techniques ........................................ 65
2. 7. 4 Blacklist/ Hotlist Management ................................................................ 66
2. 7. 5 Case Management.................................................................................... 66
2. 7. 6 Reporting and Measurement.................................................................... 67
2. 7. 7 Why do Operators Need Fraud Categorization and Reporting.......................... 67
2. 7. 8 Detection Approach – Fraud Risk Assessment............................................ 68
2. 7. 9 Best Practice Fraud KPIs – Postpaid ........................................................ 68
2. 7. 10 Prevention Measures.............................................................................. 69
2. 7. 11 Focus on Loss Prevention....................................................................... 70
2. 7. 12 Fraud Risk with New Product and Services .............................................. 70
2. 7. 13 Evaluating New Products and Services ..................................................... 71
2. 7. 14 Effective Measures – Detect and Protect.................................................... 71
2. 7. 15 Fraud Management Methodology in Developing Countries ........................... 72
2. 7. 15. 1 Start up Operator ............................................................................. 72
2. 7. 15. 2 Established Operator......................................................................... 73
2. 7. 15. 3 Best Practice ................................................................................... 73

**CHAPTER [3]: RELATED WORK ............................................... 75**

**CHAPTER [4]: JAWWAL PROFILE............................................... 86**
4. 1 Development timeline of Jawwal........................................................... **87**
4. 2 Jawwal subscribers and market penetration rate....................................... **90**
4. 3 Postpaid and prepaid subscribers ........................................................... **92**
4. 4 Jawwal revenues.................................................................................. **93**
4. 5 Jawwal anti fraud section operations ...................................................... **94**
4. 6 Jawwal bad debit.................................................................................. **95**

**CHAPTER [5]: METHODOLOGY ................................................ 96**
5 . 1 Research methodologies........................................................................ **97**
5 . 2 Questionnaire content........................................................................... **100**
5 . 3 Content Validity of the Questionnaire ..................................................... **101**
5 . 4 Statistical Validity of the Questionnaire .................................................. **102**

**CHAPTER [6]: DATEA ANALYSIS AND DISCUSTION .............106**
Research Hypothesis.................................................................................. 136

CHAPTER [7]: CONCLUSION AND RECOMMENDATION ........162

Conclusion ........ 163

Recommendation ........ 163

References ........ 165

Annexes ........ 175

# LIST OF TABLES

| No | Title of Table | Page No |
|---|---|---|
| 1. | Fraud detection/prevention literature overview | 82 |
| 2. | Palestine cellular subscribers | 90 |
| 3. | Jawwal and Wataniya market shares | 91 |
| 4. | Jawwal's lines breakdown | 92 |
| 5. | Jawwal revenues (2007-H1 2010) | 93 |
| 6. | Jawwal bad debit up to December 2008 | 95 |
| 7. | Properties of the samples | 97 |
| 8. | Department/section | 98 |
| 9. | Experience of the respondents | 99 |
| 10. | Qualifications of respondents | 99 |
| 11. | Age Group of the respondents | 100 |
| 12. | The correlation coefficient between each paragraph in the field and the whole field (Fraud detection on net of JAWWAL companies) | 102 |
| 13. | Split-Half Coefficient method | 104 |
| 14. | Reliability Cronbach's Alpha | 105 |
| 15. | The importance of anti fraud section | 107 |
| 16. | The most important step to stop fraud | 108 |
| 17. | The Fraud affect | 109 |
| 18. | The main impact of fraud attacks | 110 |
| 19. | How fraud cases are discovered | 111 |
| 20. | The bad debit resulting from fraud | 112 |
| 21. | The subscriber's fraud motivation | 112 |
| 22. | Fraud awareness writhen Jawwal company | 114 |
| 23. | Jawwal employee | 115 |

| No | Title of Table | Page No |
|---|---|---|
| 24. | The sales personnel | 116 |
| 25. | The numbers of fraud cases which are discovered and detected | 117 |
| 26. | How the insolvent customer differs from fraudulent customer? | 117 |
| 27. | The fraudulent customer | 118 |
| 28. | How the customer consider fraudulent? | 118 |
| 29. | The current criteria to identify the fraudulent | 119 |
| 30. | How fraudulent customer can be identified | 120 |
| 31. | The sales target is consider a window of fraud attacks | 120 |
| 32. | The dealers are consider a window of fraud attacks | 121 |
| 33. | The policies and procedures | 122 |
| 34. | The accelerate modifying of policies and procedures | 123 |
| 35. | Promotions and campaigns | 123 |
| 36. | Current fraud detection tools | 124 |
| 37. | The fraud management system | 124 |
| 38. | Billing reports | 125 |
| 39. | The black list window | 126 |
| 40. | The information regard fraud attacks from recourse like (complaints-call center-sales-provisioning) | 127 |
| 41. | The documents in new superscriptions and agreements | 127 |
| 42. | The services activated by default | 130 |
| 43. | The guarantee policy | 130 |
| 44. | The pricing policy | 131 |
| 45. | The most service consider vulnerable to the fraud attacks | 131 |
| 46. | The increasing number of fraud attacks in Gaza region | 132 |
| 47. | The increasing number of fraud attacks in corporate department | 133 |

| No | Title of Table | Page No |
|---|---|---|
| 48. | The most efficient way to detect fraud | 133 |
| 49. | Collaborative efforts between some destinations like (paltel-banks) | 134 |
| 50. | Chi square test (The importance of anti fraud section * number of fraud cases which are discovered and detected) | 136 |
| 51. | Chi square test (The importance of fraud * the kind of fraud attacks) | 137 |
| 52. | Chi square test (The importance of fraud * the effects of fraud) | 138 |
| 53. | Chi square test (The number of fraud cases which are discovered and detected * the current criteria to identify the fraudulent) | 139 |
| 54. | Chi square test (The number of fraud cases which are discovered and detected * Current fraud detection tools) | 140 |
| 55. | Chi square test (Current fraud detection tools * The fraud management system) | 141 |
| 56. | Chi square test (Current fraud detection tools * billing reports) | 142 |
| 57. | Chi square test (Current fraud detection tools * the black list window) | 143 |
| 58. | Chi square test (The fraud attacks * sales target) | 144 |
| 59. | Chi square test (The fraud attacks * The sales personnel) | 145 |
| 60. | Chi square test (The fraud attacks * other resource of information regarding fraud cases) | 146 |
| 61. | Chi square test (The fraud attacks * The policies and procedures) | 147 |
| 62. | Chi square test (The fraud attacks * promotions and offers) | 148 |
| 63. | Chi square test (The fraud attacks * The guarantee policy) | 149 |
| 64. | Chi square test (The fraud attacks * The accelerate modifying of policies and procedures) | 150 |
| 65. | Chi square test (The steps of fraud detection * the new subscription and agreement documents) | 151 |
| 66. | Chi square test (The fraud attacks * Jawwal employee) | 152 |
| 67. | Chi square test (The fraud attacks * The fraudulent customer) | 153 |
| 68. | Chi square test (The fraud attacks * criteria of defending the fraudulent) | 154 |

| No | Title of Table | Page No |
|---|---|---|
| 69. | Chi square test (The fraud attacks * The most service consider vulnerable to the fraud attacks) | 155 |
| 70. | Chi square test (The fraud attacks * corporate department) | 156 |
| 71. | Chi square test (The fraud attacks * The services activated) | 157 |
| 72. | Chi square test (The fraud attacks * The pricing policy) | 158 |
| 73. | Chi square test (The fraud attacks * the insolvent customer) | 159 |
| 74. | Summary about Hypothesis | 160 |

# LIST OF FIGURES

| No. | Title of Figures | No. |
|---|---|---|
| 1. | Methodology flowchart | 8 |
| 2. | Fraud management's methodology in developing countries | 74 |
| 3. | Jawwal anti fraud section operations | 94 |

# CHAPTER [1]

# INTRODUCTION

**1. 1 Background to the Study**

**1. 2 Difficulties in Detecting Fraud**

**1. 3 Definitions of Terms to be Used in the Research**

**1. 4 Statement of the Problem**

**1. 5 Research Variables**

**1. 6 Objectives of The Study**

**1. 7 Importance of The Study**

**1. 8 limitations of The Study**

**1. 9 Research Design**

1. 1 Background to the Study:

Fraud is as old as humanity itself (Bolton and Hand, 2002), and can take unlimited variety of forms. It occurs in so many areas, for example, telecommunication fraud, credit card fraud, internet transaction fraud, e-cash fraud, insurance fraud and healthcare fraud, money laundering, intrusion into computers or computer networks. The task of detecting fraud is similar in all these areas

Fraud is different from revenue leakage. Revenue leakage is characterized by the loss of revenues resulting from operational or technical loopholes where the resulting losses are sometimes recoverable and generally detected through audits or similar procedures. Fraud is characterized with theft by deception, typically characterized by evidence of intent where the resulting losses are often not recoverable and may be detected by analysis of calling patterns.

The Communications Fraud Control Association conducted a survey and determined that $72–$80 billion in losses are due to telecom fraud worldwide (CFCA, 2009). While many large operators have developed sturdy, Fraud Management Systems (FMS) to combat fraud, others have not. The Forum for International Irregular Network Access FIINA concluded that perhaps only about 10% of operators worldwide have set in place sensible and effective fraud strategies (Shalton, 2003).

The motivation behind crime is attributed to migration and demographics, penetration of new technology, staff dissatisfaction, the ‘challenge factor’, operational weaknesses, poor business models, criminal greed, money laundering and political and ideological factors (Brown,2005).

## 1. 2 Difficulties in Detecting Fraud:

a. Detecting fraud is a challenging task and is a continuously evolving discipline. Whenever it becomes known that one detection method is in place, the fraudsters will change their tactics and try others. For example, on an industrial scale, telecommunication fraud is mainly perpetrated by organized criminal gangs, professional hackers and service providers own employees (Johnson, 2002).

b. The existence of complex patterns in the customer records due to the business dynamics of each individual customer and variations among customers. telecommunication’s customer records usually include multivariate attributes, such as a customer’s usage, originating and destinating phone numbers, etc. These records are often contaminated by seasonality and/or holiday effects and the impact of marketing campaigns, which increase the difficulty of analysis and detection.

c. The development of new fraud detection methods is made more difficult by the fact that the exchange of ideas in fraud detection is severely limited. It does not make sense to describe fraud detection techniques in great detail in the public domain as this give criminals the information that they require in order to evade detection. Datasets are not made available and results are often censored, making them difficult to access Bolton and hand (as cited in Nelsson,2009).

d. Also many companies do not choose to report fraud for fear of undermining customer's confidence for the security of their own services; hence fraud is often swept under the carpet as ’bad debt’.

e. The availability of numerous hacking tools on the internet makes telecommunication fraud a wide spread crime that can be committed by anybody using various methods/means depending on one’s individual goal (Jacob, 2002). The main motivation to commit telecommunication fraud is to make money (revenue fraud), for example, by selling fraudulently obtained telephone services at cheap rates. Other motivations are non-revenue fraud, for example, by avoiding or reducing payment of services used, demonstrating ability to outmaneuver the service provider’s system security (Johnson, 2002).

## 1. 3 Definitions of Terms to be used in the Research:

### 1. 3. 1 Telecommunication Fraud:

Telecommunication fraud can be defined as the theft of services or deliberate abuse of voice or data networks (Jakob, 2002). Telecommunication fraud can be broken down into several generic classes, these classes describe the mode in which the operator was defrauded, for example, subscription using false identity. Each mode can be used to defraud the network for revenue based purposes or non-revenue based purposes. Most of these frauds are perpetrated either by the fraudster impersonating someone else or technically deceiving the network systems (Apri, 2004).

### 1. 3. 2 Bad Debts:

Bad debt occurs when payment is not received for goods/services rendered. This is, for example, in a telecommunication company, where the callers or customers appear to have originally intended to honor their bills but have since lost the ability or desire to pay. If someone does not pay their bill, then the telecom company has to establish if the person was fraudulent or was merely unable to pay.

### 1. 3. 3 Revenue Assurances:

Is a niche business activity most commonly undertaken within businesses that provide telecommunication services. The activity is the use of data quality and process improvement methods that improve profits, revenues and cash flows without influencing demand. This was defined by a trade market forum working group based on research documented in its revenue assurance technical overview.

### 1. 3. 4 Fraud Prevention:

Fraud prevention describes measures to avoid fraud to occur in the first place **(**Bolton and Hand (as cited in Nelsson, 2009)

### 1. 3. 5 Fraud Detection:

Fraud detection refers to the attempt to detect illegitimate usage of a communication network by identifying fraud as quickly as possible once it has been committed Bolton and Hand (as cited in Nelsson, 2009)

## 1. 4 Statement of the Problem:

Controlling telecommunications fraud has long been a priority in the telecom sector. The problem of fraud requires constant attention if it is to be dealt with effectively, particularly in today's radically changing telecom landscape.

In our case, the researcher will discuss what Jawwal company need to review with their fraud-management strategies and measures in order to minimize the operators' exposure to fraud.

## 1. 5 Research Variables:

a. Dependent variable is the fraud attacks on Jawwal operator

b. Independent variables are the followings:

   i. Jawwal sales target

   ii. Jawwal programs policies and procedures

   iii. Current prevention and detection tools

   iv. Fraudulent method.

   v. Employee's awareness of the fraud problem.

## 1. 6 Objectives of the Study:

a. General objective: To focus on how Jawwal company managing and detecting the fraud.
b. Specific objectives:

   i. Providing the way to protect the Jawwal brand image, assets and revenue streams from loss through internal and external fraud and other forms of illegal activity.

   ii. Develop strategies, policies and guide lines that enable a continuous cycle of detection, monitoring, investigation and prevention for fraud management.

   iii. Create a fraud and security awareness culture across Jawwal.

## 1. 7 Importance of the study:

Fraud remains serious global issue for mobile network services despite improvement in security technology. While recent development have enhanced some capabilities and filled known security holes, fraudsters have been nimble enough to seek alternative techniques that minimize detection with current technologies, so there is great need of high awareness in facing fraud phenomena.

Another importance of the research, it's focusing on fraud threads directing to telecom operators, due to the fact that there are not enough studies that focusing on fraud generally and fraud detection in cellular communications especially throughout the operators working in the Arab region.

## 1. 8 limitations of the study:

a. As telecommunication fraud is widely spread, this is a wide area for the thesis, therefore; the researcher will limit the study on fraud management in telecom cellular network, and will not cover the issues related to fixed line telephone networks, using one of the telecommunication service providers, Jawwal Company as case study.

b. There is some restriction from Jawwal company regard the amount of bade debit and live examples of fraud attacks

c. There is limited recourses about telecom fraud management in the operators working in the Arab regions

## 1. 9 Research Design:

The first phase of the research thesis included identifying and defining the problems and establishment objective of the study and development of the research plan.

The second phase of the research included a summary of the comprehensive literature review. Literatures on fraud management were reviewed.

The third phase of the research included a field survey which was conducted about the fraud detection on Jawwal Company, the research focused on the modification of the questionnaire design, through distributing the questionnaire to pilot study, The purpose of the pilot study was to test and prove that the questionnaire questions are clear to be answered in a way that help to achieve the target of the study. The questionnaire was modified based on the results of the pilot study.

The fourth phase of the research focused on distributing questionnaire. This questionnaire was used to collect the required data in order to achieve the research objectives.

The fifth phase of the research was data analysis and discussion. Statistical Package for the Social Sciences, (SPSS) was used to perform the required analysis.

The final phase includes the conclusions and recommendations.

A two hundreds questionnaires were distributed to the research population and (170) questionnaires are received.

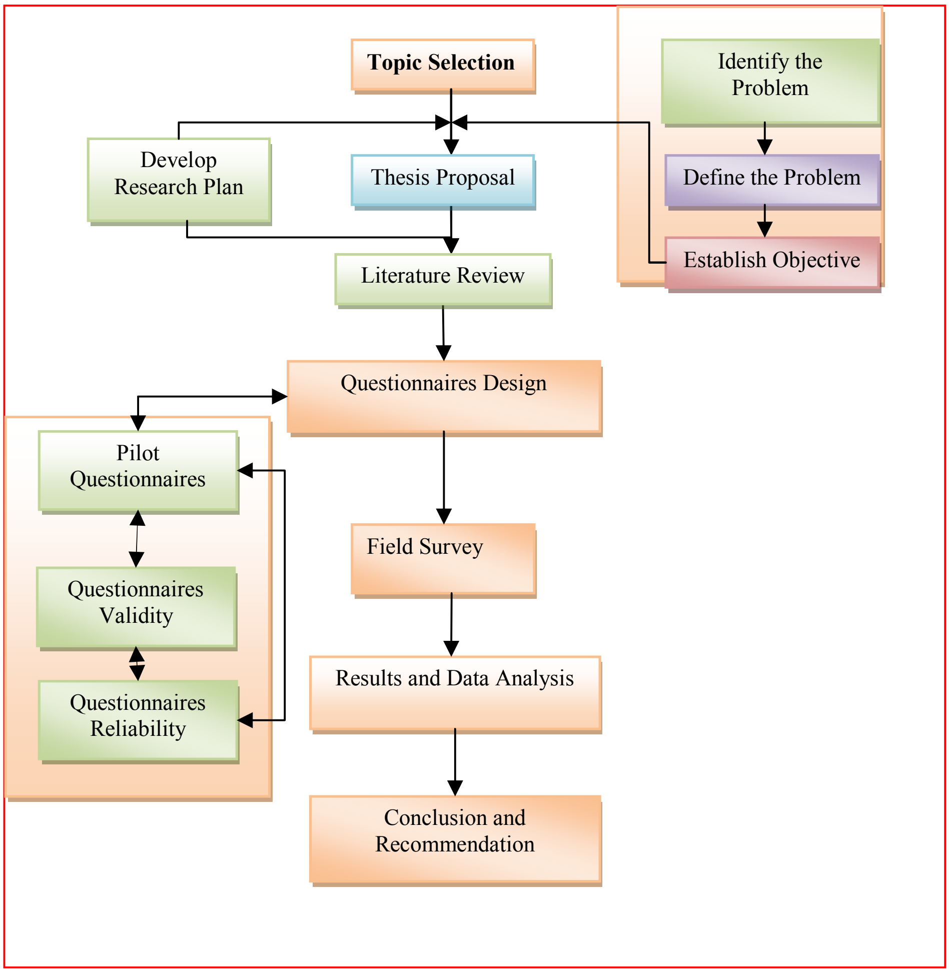

***Figure (1) methodology flowchart***

## CHAPTER [2]

# LITERATURE REVIEW

**Section 1: Telecom Fraud Overview**

**Section 2: What Makes People Perpetrate the Fraud?**

**Section 3: Which are the Most Prevalent Fraud Types that are Occurring?**

**Section 4: Which are the Likely Products and Services to be Attacked?**

**Section 5: What is the Source of Information to Facilitate the Fraud?**

**Section 6: How are Fraudsters Perpetrating the Fraud?**

**Section 7: Detection and Prevention**

## SECTION 1: TELECOM FRAUD OVERVIEW

**2. 1. 1 What is Telecom Fraud?**

**2. 1. 2 Some Recent Figure about Telecom Fraud**

**2. 1. 3 Some Factors Leading to Telecom Fraud**

**2. 1. 4 Where doe's Fraud Exists?**

**2. 1. 5 Does Fraud Differ by Geography?**

**2. 1. 6 How Much Damage is Fraud Doing?**

**2. 1. 7 What is the Real Cost of Fraud?**

**2. 1. 8 Fraud Positioning Approaches**

**2. 1. 9 Fraud Management Approaches**

**2. 1. 10 What's the Difference Between a Fraud and a Bad Debt?**

### 2. 1. 1 What is Telecom Fraud?

Many definitions in the literature exist, where the intention of the subscriber plays a central role. Johnson defines fraud as any transmission of voice data across a telecommunications network, where the intent of the sender is to avoid or reduce legitimate call charges Johnson (as cited in Hollmen, 2000). In similar vien, Davis and Goyal , define fraud as obtaining unbuildable services and nude-served fees (as cited in Hollmen,2000). Hoath considers fraud as attractive from fraudster's point of view, since detection risk is low, no special equipment is needed, and product in question is easily converted to cash (as cited in Hollmen, 2000). Although the term fraud has particular meaning in legislation, this established term is used broadly to mean, misuse, dishonest intention or improper conduct without implying any legal consequences.

### 2. 1. 2 Some Recent Figure about Telecom Fraud:

Fraud is a problem for all businesses (KPMG's, 1998), it is generally internal or external or a combination (collusion), (Katz, CFE and CFS, 2010). Increased innovation in telecoms fuels more fraud also increased competition provides more avenues of attack, increased mobility also means fraudsters are harder to track down and internationally organized.

In survey conducted by communication control fraud association (CFCA), including 123 operators and more than 30 countries, the survey estimated the global fraud loss as the fowling (Kumar, 2010):

a. 72$-80$ billion (USD) annually (34% increase from 2005

b. Approx.4.5% of telecom revenue

c. 91% global fraud losses increased or stay the same

d. Top 3 fraud types:

    i. 22$ billion-subscription fraud/Identity (ID) theft

    ii. 15$billion –compromise private branch exchange (PBX)/voice mail system

    iii. 4.5 $ billion –premium rate service (PRS) fraud

### 2. 1. 3 Some Factors Leading to Telecom Fraud (Sanwalka, 2010):

a. How the technology is actually installed and configured, default settings.

b. How the technology, products and services are sold /offered

c. Inherent weaknesses in procedures and working practices

d. Lack of management control, supervision and monitoring

e. Lack of knowledge and experience of personnel

f. Rush to market - no product or service fraud risk evaluation

### 2. 1. 4 Where Doe's Fraud Exists?

Fraud exists in every operator in every country throughout the world there is no exceptions, committing fraud does not need highly complex equipment or skills, fraudsters are normally lazy people. Fraudulent application for service is the first step in achieving illegal access to network services, Fraudsters prey on operator's weaknesses in their controls and procedures. In a recent survey 85% of the communications operators surveyed stated that global fraud losses have increased or stayed the same.(CFCA,2006), all operators will suffer from some internal fraud at some point irrespective of whether they believe their employees are all honest and trustworthy (KROLL, 2009).Top 5 Countries where fraud was concentrated were Pakistan, Philippines, Cuba, India and Bangladesh, Cuba being the newest member to the t op 5 lists (CFCA,2006)

### 2. 1. 5 Does Fraud Differ by Geography?

On a geographic basis, operators in Middle East and Africa suffered most, experiencing more than 20% losses, while Asia close behind at just below 20% and Central America and Latina America at more than 15%. Western Europe ranked lowest in losses at about 7%, following by Central and Eastern Europe 8% and North America just about at the average at 13%, (chau,2007), so Is fraud different here (Palestine) than other countries? The answers may be no, or yes:

a. NO: A subscription fraud is a subscription fraud where ever in the world.

b. YES: Local culture and sales offerings, method of activation etc. … may mean the techniques used by the fraudster will be different.

c. Primary Fraud Types are common and we will cover these in detail in the research: Subscription, internal. Dealer, Technical etc...

d. Many secondary Techniques are the same: Call Selling, Roaming, PRS, Bypass

e. Some techniques will be unique to a specific marketplace

### 2. 1. 6 How Much Damage is Fraud Doing?

No one really knows how much fraud is costing the industry with estimates varying considerably:

a. Unpaid bills and defaulting customers are costing mobile operators around US$26 billion every year with around 5% of total billings being written off annually (cellular-news, 2006).

b. The Communications Fraud Control Association (CFCA, 2009) estimated that annual global fraud losses in the telecoms sector were no between $54 billion and $60 billion, an increase of 52 percent from previous years.

c. The CFCA also estimated that global annual losses to fraud account for 5 percent of the total telecom sector revenue with mobile operators seen as more vulnerable than fixed line.

d. 47.3% of global fraud losses are from Subscription/ Identity Document (ID) Theft and Private Branch Exchange PBX/Voicemail (CFCA, 2006).

### 2. 1. 7 What is The Real Cost of Fraud?

Fraud losses continue to impact virtually every business enterprise, despite significant advances in fraud detection technology, fraud losses continue to pose a significant problem to many finance, insurance, health care, internet merchants, brokerage and securities, and many other, about the telecom companies We can only estimate the cost because operators are reluctant to admit to fraud or are not actively looking for fraudulent accounts in the bad debt (GOLIAT, 2004),also the business driver is for subscriber growth and market share, therefore, the fact that huge number of the new customers could actually be fraudsters is not taken into consideration. Responsibility for chasing unpaid bills is spread across a variety of departments which could include billing, IT, fraud, credit management, customer service, collections and the finance departments, this often results in an ineffective ability to collect debts and a1so does not help identify fraud as skills are not present in all business areas to identify fraudsters as opposed to bad debtors (federal register, 2008).

Networks do not or cannot distinguish between fraud and bad debt (Business issue, 2009).Prepaid ,internal and interconnect/bypass fraud is rarely included in the reported figures Areas unrelated to airtime loss are not included such as theft, subsidy and commission payments and the cost of customer acquisition etc (nokia siemens network, 2008).

In deregulated markets and with mobile phones often replacing fixed lines, the threat of disconnection is no longer as strong as it was, the fraudster can simply move network if they are disconnected, therefore, the operator is more reluctant to cut a customer off in case they were not actually a fraudster for fear of losing customer numbers.

### 2. 1. 8 Fraud Positioning Approaches:

Where does fraud actually fit into the business? There are different approaches worldwide. Fraud as part of the revenue assurance capability, linked with security or stand alone there is no right or wrong approach. Fraud Management is about minimizing exposure, detecting illegal activities and implementing effective controls so that fraud is harder to perpetrate in the future (Graycar and smith,2002). Fraud Management is about making the network and business operations safer, ensuring top management that the fraud phenomenon is understood and being kept under control. Objectives of fraud management are easier to understand and to "sell" to the business than other aspects of risk management..

Fraud Management will detect and prevent fraudulent activities in all areas under its remit, operate in line with the powers mandated by executive management, act quickly on discovered instances of fraud to stem losses ,produce effective controls, monitoring capabilities and preventative actions in order to diminish the exploitation risk measure, report on and escalate issues and track the resolution when appropriate. Fraud management is not a collection or credit control department nor an internal audit department (Graycar and smith,2002).

## 2. 1. 9 Fraud Management Approaches:

When it comes to fraud management, operators must think about answers for the following questions:

a. What is the remit, roles and responsibilities, varies considerably depending on the geographic region? Operator/market maturity and level of fraud capabilities externally i. e. organized frauds.

b. What does executive management mandate as fraud responsibilities?

c. What are the resources available, skills levels, capabilities and experience of handling telecoms and none telecom fraud?

d. What tools can they use? (In house developed or commercial fraud management system FMS).

e. What experience they have. And what is the analysts' background?

f. What are the company priorities? Stem losses. Protect customer and/or company reputation etc.

While a lot simpler to implement, there are various models regarding fraud management activities (Kenneth, 2004), Praesidium, an established communications risk Management consultancy, specializing in telecoms Fraud Management have witnessed some FM models approaches (Robert and Dabija, 2009).

### *2. 1. 9. 1 FM Approach 1:*

Mobile Operator with 5 million postpaid, 7 million prepaid customers, offering whole range of Mobile services, fraud team is made of25 analysts; they work together with credit and collection teams, a total of 55 analysts. Remit is purely subscriber and dealer fraud, they work 24 hrs shifts. All teams (Fraud, Credit, and Collection) have access to FMS and various reports, background is customer service, limited technical knowledge, and significant staff chums. The advantages of this approach is the huge staff and resources, big detection potential, the disadvantages on the other hand is remit is unclear, so same tools are used for fraud and credit management , high level of false alerts , FMS is for fraud not bad debt management and there is no specific experience or specialization in purely fraud detection , low level of accurate targeting and essentially number crunching , increased level of risk from providing access to confidential information to large staff numbers

### 2. 1. 9. 2 FM Approach 2:

Mobile operator with 3 million postpaid, 12 million prepaid customers, offering whole range of Mobile services ,fraud team consists of fraud manager and 7 analysts investigations manager and extra 5 fraud specialists ,thorough investigations of subscription frauds, up to arresting and filing the case to the court - legal action ,no FMS reliant on internally generated reports and notifications, background is customer service, technical security, financial fraud, the advantages of this approach is experienced and specialized staff , mixed and solid combination of skill sets, multi disciplined team with different abilities and knowledge of the business on the other hand the disadvantages are, manual intensive tasks, huge level of paperwork, time consuming, leaves large amounts of fraud cases not dealt with (inability to priorities) ,focus mainly on subscription fraud, spending months investigating it , low return in value and Reasonable Operator Initiative of the function, staff morale decreasing due to poor perception in the business .

### 2. 1. 9. 3 FM Approaches 3:

Fixed Line operator with 25 million customers, 400K payphones **,**fraud tam is made of head of fraud and 4 analysts ,ex engineers ,remit is all subscribers, dealer and partner fraud ,FMS and reports in place ,background is Engineering, Marketing, and Finance, this approach advantages are good mixture of qualities and experience, practical approach to fraud , high level of results ,high ratio of investigated versus fraud detected, and focused on big fraud hitters. The disadvantages on the other hand are ,low level of staff and resources in comparison to level of exposure fraud increasing due to launch of new untested services (not in remit) , and FMS primarily used for detecting the known frauds and not being used to detect a new services and products .

### 2. 1. 9. 4 FM Approach 4:

Fixed line and global system for Mobile communications GSM operator with 10 million customers. 50K payphones, fraud team consists of fraud manager and 6 Analysts. Background is Information technology/Internet protocol, Engineering, and financial and commercial FMS available. Also management reports and key Performance Indicators (KPls) in place, remit is subscriber, dealer and partner fraud, and internal fraud. product risk assessments, background is engineering, marketing, finance, customer care, business analysts, the approach advantages are good mixture of skills, qualities and large coverage of fraud areas, remit and requirements is clear and supported by tools and experienced, trained resources, high ratio of investigated versus fraud detected and one disadvantage is areas overlapping with other departments, needs careful management.

### 2. 1. 10 What's the Difference Between a Fraud and a Bad Debt?

**Simple Rule about Fraud and Bad Debt** (GOLIAT, 2004)**:**

Fraudsters have no intention of paying the bill from the day they take out service, deceive the operator, they are dishonest, liars, and fraud is based on the intention, on the other hand bad debtors intended to pay when they took out service, however, for various reasons no longer have the means to pay, and they usually only "do it" once and fraudsters repeatedly offend (multiple applications, different names, across different operators etc).Bad debtors can, however, become fraudsters, when they realize that they no longer have the means to pay so will 'abuse' the service to the limit knowing they no longer intend to pay.

#### *2. 1. 10. 1 Effects and Impact of Bad Debt:*

Bad debt has a direct cost to the company its levels vary from operator to operator, seen instances of levels at 18-20% of revenue, good levels are <1% or averaging 1-3%.(Hale, 2010).

Some operators looking to increase postpaid customer growth and migrate prepaid to postpaid - loyalty programs. This approach will require greater focus on credit control capabilities as levels of bad debt could increase.

#### *2. 1. 10. 2 Effects and Impact of Fraud:*

Fraud has a cost to the company often hidden, until it's too late. Fraud is classed as an act that causes intentional or deliberate revenue loss or other damage against a company. Fraud not only causes revenue loss but can result in (Levi, Burrows, Fleming, Hopkins and matthews, 2007):

a. Increases in the operators operating costs.

b. Increase in prices to the customer.

c. Bad publicity.

d. Share price fluctuation.

e. Low morale, especially where internal fraud is involved

f. Loss of jobs.

g. Litigation and consequential financial loss.

h. Loss of service and inability to dispense contractual obligations.

i. Regulatory fines or increased regulatory supervision.

## SECTION 2: WHAT MAKES PEOPLE PREPERATE THE FRAUD

2. 2. 1 Who Actually Commits Fraud?

2. 2. 2 Where Do Fraudsters Work From?

2. 2. 3 Why Do Fraudsters Do It?

2. 2. 4 Some Motivation For Committing the Fraud

### 2. 2. 1 Who Actually Commits Fraud?

a. Fraud has and can be committed by any type of person in society Albrecht, cherrington, payne ,Roe and Romeny (as cited in anonmyous,2003.p 18), whatever the social status, nationality, or position/role within the business, If they have the driver (initiative, desire. Commitment, purpose etc) they will find the way and means to commit fraud, no one is exempt.

b. Bernard Ebbers, the former Chief Executive Officer (CEO) of Wor1dCom. Was sentenced to 25 years in Jail for orchestrating an $11 billion fraud.(Bayot,2005)

c. Berard Maddoff, non executive chairman at NASDAQ stock exchange, commits the largest financial fraud in history, with losses estimated at $65 billion based on a 'Ponzi Scheme"- a pyramidal build up. Leading to inevitable collapse. He has been convicted and sentenced.to150 years in prison.(Gagnier,2009)

Company managers were named as the biggest perpetrators in a recent fraud survey as they are often not being watched, they are trusted and have access to more information and systems than other employees under them. (Robert and Dabija, 2009)

### 2. 2. 2 Where Do Fraudsters Work From?

External fraudsters can work from anywhere as they often have people working for them whilst they control the fraud activities centrally, often they will pay for personal details, identity documents, or pay other people to obtain subscriptions for them in their name to avoid detection "The end justifies the means"(NAO, 2008). Roaming frauds are committed outside of the home network with either the fraudster or their contacts being in another country running the fraud, they cross international boundaries, operate globally (GSMA, 2008). Hackers can work from anywhere there is internet access, unlimited opportunities provided by technology, internal frauds committed from inside the company often with outside collusion and influence, far easier to commit from within (NAO, 2008).

### 2. 2. 3 Why Do Fraudsters Do It?

a. Incentive - What does the fraudster expect to receive for committing the crime, easy money with minimal risk?

b. Opportunity - Can the fraudster successfully commit the crime and get away with it. Lack of adequate supervision of activities, weak Internal controls, no accountability, and ineffective audits present opportunities for the fraudster.

c. Rationalization - Fraudsters believe they can commit their crimes and their actions are justified. They do not live by the same acceptable norms and standards of society. They commit fraud simply because they can and do not care about their victims.

d. Capability - The fraudster must have the requisite education, skills, knowledge, expertise and experience to be capable of effectively committing the fraud.

### 2. 2. 4 Some Motivation for Committing the Fraud (Bihina Bella, Oliver, Ellof, 2005)

#### *2. 2. 4. 1 Financial Gain:*

a. Profit by not paying for their own airtime usage: Free/reduced cost communications - either by subscription or internal fraud.

b. Profit by selling the airtime to others (call selling): A competing business, offering calls/data at a cheaper price than the network.

c. Profit from selling the Subscriber Identity Module (SIM) cards: Can be easily delivered globally by an express courier service.

d. Profit from selling equipment i. e. handsets: Can be exported to other countries where they will command a high price, especially if the phone was subsidized on the home network.

e. Financial gain from internal frauds.

#### *2. 2. 4. 2 Revenue Fraud:*

Revenue Fraudsters look for:

a. High value service offerings - roaming, international access etc.

b. High volume/multiple SIMs a/lowed on an account.

c. Subsidized equipment or the ability to pay for the equipment on the first invoice, over the term of the contract or by credit card, enables an ability to deploy delaying tactics.

d. Ability to have roaming and international direct dialing (IDD) activated at the point of sale, no deposits or restrictions.

e. Weaknesses in the registration process, lack of bad debt management, blacklists, default account management etc.

f. Length of time until they are detected and service is terminated.

### *2. 2. 4. 3 Anonymity:*

a. Avoid detection by network operator, police and authorities as the 'real' user of the service is unknown.

b. Prepaid and now Voice over Internet Protocol (VOIP) is often used by criminals as subscriber details are unknown and call records are not easily obtainable for analysis purposes, activities not easily traceable.

c. Nuisance (cramming and slamming), call issues, not directly fraud related but sometimes handled by Fraud Departments.

d. Increase in law enforcement liaison - other criminal activity (organized crime, terrorism, drug dealing, VAT scams etc).

e. Global fraud losses have risen due to an increase in worldwide terrorism.

f. Terrorist organizations embrace communications fraud to generate funds by illegally gaining access to a network and then reselling the service and to remain anonymous.

### *2. 2. 4. 4 Lack of legislation and prosecution:*

a. The penalties for Telco related fraud are typically less severe than for other criminal activity.

b. Most countries are only now looking at specific telecoms related legislation, therefore no actual deterrent.

c. Operators struggle to proceed to a successful prosecution, with cases taking many months or even years to go to court.

d. The cost of investigating the incident, subsequently identifying the fraudster is far higher than the potential for recovery of monies

e. In general defrauding operators is, therefore, a relatively low risk and lucrative activity, quick and easy money.

f. It is no wonder that some gangs now see it as more profitable than drug smuggling.

## SECTION 3: WHICH ARE THE MOST PREVELANT FRAUD TYPES THAT ARE OCCURING

**2. 3. 1 Subscription Fraud**

**2. 3. 2 Usage/ Airtime Fraud**

**2. 3. 3 Unauthorized Service Fraud**

**2. 3. 4 Sales and Dealer Fraud**

**2. 3. 5 Technical Frauds**

**2. 3. 6 Internal Frauds**

**2. 3. 7 Equipment Frauds**

### 2. 3. 1 Subscription Fraud:

Subscription fraud is being experienced by all operators; it is oldest type of telecom fraud, indeed one of the oldest types of fraud in any business environment (Yates, 2003). Also it considered as one of the most commonly suffered frauds by operators and accounts for most of their secondary losses, it is airtime related, another thing should be mentioned it is a procedural, not technical fraud, looks for weaknesses and exploits them. The Subscription fraud result looks like bad debt and is often misinterpreted as bad debt, It is estimated that 70% of fraud losses relate to subscription fraud which is over $28 billion a year (78 million dollars a day!). (NFA, 2010)

### 2. 3. 2 Usage/ Airtime Fraud:

One of the most common forms of fraudulent attack, as it generates substantial revenue for the fraudster, it is contributes significantly to a telecoms losses, cost of home traffic, IDD, Interconnect costs, the exposure increases substantially. Basically the volume of phone calls will increase over times which are later not paid for, it simple, effective and results in a direct financial loss (Yates, 2003).

### 2. 3. 3 Unauthorized Service Fraud:

The use of a product or service without authority, this can be committed by a third party with no direct contact with either the customer or the company. Often only identified when it is too late, or advised by the genuine customer (B/OSS, 2004).

### 2. 3. 4 Sales and Dealer Fraud (Johnson, 2002)

a. Subscription fraud, does occur from operators own sales channels (dealers, sub dealers, operators own sales outlets etc).

b. Commission fraud - linked to sales and dealer fraud as it simply means extra money.

c. Bonuses - for reaching sales targets or selling specific services.

d. Theft of equipment - handsets, accessories, vouchers etc from stock.

e. Prepaid vouchers - some are even sold at higher than face value in remote areas (supply and demand).

f. Box splitting - normally associated with selling component parts of prepaid offerings (handset/SIM/voucher/commission etc).

### 2. 3. 5 Technical Fraud:

More advanced fraud that is based in exploiting loopholes found in the operator network element or platforms base stations, some types of technical fraud as follows (Brown, 2005):

a. Switching/signaling.

b. Home Location Register (HLR)/ Authentication Center (AUC).

c. Mediation.

d. Billing.

e. IT, Local Area Network (LAN), Wide Area Network (WAN).

f. Internet.

g. Intranet.

h. Cloning.

### 2. 3. 6 Internal Fraud:

Unfortunately it's taking place everywhere, as product and service advancements increase the requirement to come inside the company will also increase. All areas of the business are exposed and vulnerable; everything has a value and a price, including loyalty. Technical staffs write and manage IT systems, operators have to control who has access and to what purpose, the operators also must fictitious suppliers and contractor, also collusion, corruption and sabotage all pose a realistic business threat. Some types of internal fraud is as follows (Brown, 2005):

a. Theft of data/equipment.

b. Network attacks abuse.

c. Employee placement.

d. Payroll.

e. Misuse of computer systems.

f. Ghosting.

g. Sale of sensitive information:

    i. Customer related information.

    ii. Products, new services and equipment.

    iii. Sales figures.

    iv. Marketing campaigns.

## 2. 3. 7 Equipment Fraud:

The manipulation of telecoms equipment to facilitate a fraudulent attack, it can be customer equipment or company equipment. Equipment fraud varies from handsets to switches, from maintenance tools to card/voucher printing machines. Also subsidy fraud is a part of this where handsets are obtained at a subsidized rate and then resold at face value in other markets usually abroad (Brown, 2005).

### *2. 3. 7. 1 Black market Phones – Examples:*

a. Globally an estimated 39 percent of all handsets sold were distributed via the black market representing a loss of USD 2.7 billion tax revenue (Cellular news, 2010).

b. India - smuggled phones are 40% cheaper than legal imports, account for about half of all handsets sold in India.

c. A Siemens AG handset costs 5, 000 rupees ($114) with the logo of Royal KPN NV, Holland's biggest phone company. The genuine cost is 9000 rupees, around 44% dearer than the smuggled phones (Robert and Dabija, 2009).

d. 38% of the wireless handsets sold in China were smuggled into the country with the handsets being accompanied by forged network certificates. The sales accounted for some $1. 2B in revenues, with each smuggled phone going for an average of $241(Robert and Dabija,2009)

e. Ericsson and Samsung are among the most popular smuggled phone brands, while Nokia, Motorola and Siemens are the top sellers through legal channels.

`

## ECTION 4: WHICH ARE THE LIKELY PRODUCTS AND SERVICES TO BE ATTAKED?

### 2. 4. 1 The fraudsters attacked the Weakest Link in the operator

### 2. 4. 2 What Does Get Targeted?

### 2. 4. 1 The Fraudsters Attacked the Weakest Link in the Operator:

The weakest link can be anywhere inside business processes relating to:

a. Network access.

b. Customer activation process.

c. Billing, charging process.

d. Payment options.

e. Revenue share.

f. Value Added Services (VAS) (Roaming, PRS etc).

g. Money back abuse.

### 2. 4. 2 What Does Get Targeted?

It is impossible to operate "100% risk and fraud free" so we need to consider exactly what is likely to be targeted across the different product and service offerings, fraudsters will always want feature and service rich products, the following are the products and services fraudster want to attack.

#### *2. 4. 2. 1 Fixed Lines:*

Fixed line telephony is the traditional well established telecom service. In most countries now it is very basic compared with other technologies and services, it is very easy to obtain, little customer validation takes place high percentage of the populations in most countries have access to at least 1 phone line (T W Hazeltt,2006).

#### *2. 4. 2. 2 Indirect Access (IDA):*

Generally offered by Postal Telephone and Telegraph (PTT) competitors in deregulated markets and very competitive price wise, it can use access codes or single line units (SLU) to re-direct the traffic, these can be subject to reprogramming or re routing of traffic. And in some cases customers' simply plug and play via simple connection, no direct customer contact. It can be prepaid or postpaid service. (icta authority,2003).

### *2. 4. 2. 3 Mobile:*

Mobile services have been targeted for fraud since their introduction. Fraud is no longer restricted to one place. Fraud can now travel globally, via satellite. Another thing should be mentioned that Mobile is feature rich, providing more money making opportunities to the fraudster, as technology improves and becomes more complex, so does the fraudster's knowledge (Krenker, Volk, Sedlar, Bester, and Kos, 2009).

### *2. 4. 2. 4 VOIP services:*

Service convergence is now increasing the risk, it is non geographical services mean fraudsters can be from anywhere and not always traceable, known PC vulnerabilities are now applicable to phones as well therefore increasing security risk as well as fraud exposure, finally network security is becoming of increasing importance for fraud management (thermos,2008).

### *2. 4. 2. 5 Postpaid Service:*

The most traditional service offered by operators, it is effectively providing 1-3 months credit upon taking up service, some countries adopt pre payment or payment in advance, postoaid service offers multiple payment options (cash, cheque, direct debit, credit card, etc via different outlets), it is often allowing more services than prepaid, and therefore still targeted for fraud, its' collection timeliness and costs incurred add to the operator burden and can sometimes hide the true level of fraud (bad debt), the issue relating to the postpaid service and there billing and Payment, could also create chance for the fraudster to attack the operators such as; options for different billing addresses, options for different billing cycles spread the fraud finally the ability to be added to “AN Associated Aumber- others” account - direct debit (earth vision cellular)

### *2. 4. 2. 6 Prepaid Service:*

Still extremely popular and registers continuous growth especial in developing and cash driven society, the service is easy to obtain and relatively easier to manage (earth vision cellular):

a. Lower customer acquisition cost

b. Quicker financial retune on costs

c. No personal details required/supplied

d. No contracts or formal registration process

e. No customer validation requirements

f. Prepaid Service Provides different top-up facilities

    i. Vouchers

    ii. Web based and E payment Virtual vouchers

    iii. Credit cards

    iv. ATM

    v. Cash

g. Provides anonymity for criminals

h. Increase in law enforcement issues

i. Now many similar services to postpaid - Roaming, Premium Rate Servicers( PRS),

j. General packet radio service (GPRS), Content

### *2. 4. 2. 7 Satellite:*

Allowing completely unrestricted global communications, it is expensive equipment costs, expensive call charges, it is have billing issues - ability to contact customers for billing and payment, also it have legal considerations on and investigation/jurisdiction issues (Robert and Dabija,2009). .

### *2. 4. 2. 8 Value Added Features and Services (VAS):*

Value-added services (VAS) are unlike core services, they have unique characteristics and they relate to other services in a completely different way, they also provide benefits that core services can not(pradhan,2008):

a. IDD (International Direct Dialing)

b. Call Forward.

c. Multi party calling.

d. Voicemail.

e. Short Message Service (SMS).

f. SMS to PRS.

g. Multimedia Massaging Service (MMS).

h. Fax .

i. WAP .

j. General packet Radio Service (GPRS) .

k. Third Generation (3G).

### *2. 4. 2. 9 Roaming Service:*

Allowing mobile customers to use their phone abroad, calls are not on the home network and there is no direct visibility of customer activity, the Call Detail Record (CDRs) must be sent by visited network, delays increase the fraud risk, in roaming there is high call cost, fraud risk also increasing. The inter operator relationships and responsibilities not contractually agreed for fraud management (standard contracts only), another thing is prepaid roaming now becoming more common place, finally the External Linkages( EL) protocol issues prevent accurate charging and are abused by customers. (GSM, 2008)

### *2. 4. 2. 10 Premium Rate Services (PRS):*

Premium rate services are a form of micro payment for paid for content, data services and value added services that are subsequently charged to your telephone bill. They tend to cost more than a normal phone call or text message, some of PRS characteristics are as follows (ict Qatar):

a. Revenue sharing product.

b. Telco shares profits with the information provider, Such as: Competition/prize lines. Betting information, weather reports and share prices.

c. Very high value calls charges.

d. National and International calling.

e. Single drop charges.

f. Frauds are globally prevalent and increasing especially with VoIP and roaming for International Revenue Share.

g. Losses can be considerable and fatal.

### *2. 4. 2. 11 Customer Confidential Information:* (Sanwalka, 2010)

a. Customer data bases - (personal data, names/addresses etc).

b. Account Information - (bank account details, direct debit mandates).

c. Outgoing Calls - historical and recent (sometimes indefinite).

d. Incoming Calls - recent billable events. Location Updates - identification of a person's whereabouts.

e. Billing Information - selling of information.

f. Credit Card information - selling or use of information.

### *2. 4. 2. 12 Selling of Information:*

a. UK investigators recently identified at least 22 Web sites selling unauthorized personal phone data, including cell phone roaming records, the date and time of the calls, and their origin and destination (Brookson, farreill, whithead and zumele, 2007).

b. Recent call records/SMS content being made available to unauthorized parties was registered in Cyprus and Greece, with huge impact on operators' image.

### *2. 4. 2. 13 E- Commerce Services:*

More and more operators also sell their services on the Internet, Web Shops, the customers can buy phones, accessories, top up their prepaid accounts etc.., but the customer identification and authorization are sometimes poorly controlled; and it is highly exposure due to credit card fraud, often liability resides with the operator (merchant) who is facing huge chargeback's due to fraud (can be up to 90days on international cards), in addition to chargeback's (fraudulent payments). The operators face penalties from Credit Card companies (Bihina Bella,Oliver,Ellof,2005)

### *2. 4. 2. 14 M - Commerce Services:*

On the increase with more and more services available, downloading ringtones, paying for services or subscriptions was just the beginning, research shows customers accessing banking products and services via mobiles will reach more than816million by 2011 with total transactions for M-payment growing 68% per annum reaching$250 billion in 2012. ( fierce wireless, 2008), as these services become more popular, will definitely be targeted by fraudster's (fact). A financial institution globally already have bad image due to current economic climate, Telco's cannot fall into the same category therefore requires security and trust.

### *2. 4. 2. 15 Webcare Systems:*

Customer has capability to view his invoice online, can pay his invoice via this method, can manage services, activate or deactivate accounts, view and alter payment information, view and alter credit card details. Fraudsters will use same techniques as experienced in banking fraud, Phishing for instance, to manipulate funds. Customer education is essential and critical, so are the fraud controls which should be embedded in such a system (Robert and Dabija, 2009).

### *2. 4. 2. 16 Warehouses, Dealers, Sales Outlets:*

It may be old fashioned but still cost effective for the criminal it means vulnerable premises with high value telecom stock are attractive. Thefts experienced from robberies at warehouses/sales outlets which are poorly secured or managed by 3rd parties, and thefts in transit or via the distribution process. Many operators still have minimal and poor controls around equipment (handsets. terminals. vouchers etc), these are very attractive to fraudsters who will either use force or alliteratively bribe employees to gain access to steal stock, and missing stock can go unnoticed without good inventory controls and auditing initiatives(cortesao,martins,rosa and carlho).

### *2. 4. 2. 17 Calling Card:*

A card that is used instead of cash to make telephone calls, a printed or written greeting that is left to indicate that you have visited, it contains (Bihina Bella,Oliver,Ellof,2005):

a. Personal Identification Number (PIN) compromise.

b. Account number + PIN compromise.

c. International destination calls. International originated calls.

d. Business customers are easy targets.

e. Attacks take place from airports, train stations, hotels etc

### *2. 4. 2. 18 Payphone:*

Is a public telephone, usually located in a stand-alone upright container such as a phone booth, with payment done by inserting money (usually coins), a credit or debit card, or a telephone card before the call is made, the following are the payphone characteristics (brown.2005):

a. Prime targets for fraud/crime.

b. Payphones contain cash.

c. Engineering codes compromised.

d. Boxing techniques employed.

e. Teeing in to lines.

f. Blocking.

### *2. 4. 2. 19 Private Branch Exchange (PBX):*

Private branch exchange (PBX) is a telephone exchange that serves a particular business or office, as opposed to one that a common carrier or telephone company operates for many businesses or for the general public, some characteristics of PBX" Bihina Bella,Oliver,Ellof,2005)":

a. Companies PBXs can be manipulated remotely.

b. Fraudulent calls can be hidden amongst high business usage.

c. International access frequently available.

d. Any company can be targeted, not just telecoms.

## SECTION 5: WHAT IS THE SOURCE OF INFORMATION TO FACILITATE THE FRAUD?

**2. 5. 1 Information is Power**

**2. 5. 2 Sources of Information**

**2. 5. 3 Employee Compromise**

**2. 5. 4 Sale Channels**

**2. 5. 5 Vendors**

**2. 5. 6 Media**

**2. 5. 7 Internets**

**2. 5. 8 New Generations of Networks**

**2. 5. 9 Customers**

**2. 5. 10 Suppliers**

**2. 5. 11 Competitors**

**2. 5. 12 Fraud Information Sharing**

### 2. 5. 1 Information is Power:

To operate a Telco you need "information" and this will come in many different forms and from many different sources. Information sources are used every day for the following:

a. Marketing intelligence it means competitor information.

b. Sales techniques such as advertising and new methods of distribution.

c. Technological advancements, it means staying ahead of the competition.

d. Products and services, means meeting the needs of the customer.

e. Pricing and tariffs (bundled packages), business differentiator for keeping ahead of the competitor.

f. Customer retention/chum management, means assessing customer loyalty to ensure customer growth.

The same basic principles apply to committing fraud. Fraudsters need to know, the vulnerable operator; who is too easy option. The market; who are they providing "illegal and fraudulent" service. The technology; which equipment, platforms, handsets etc are the weakest? The sales figures; How much money are they potentially going to make from their fraud? The products and services; meeting the needs of their customer base. Pricing and tariffs (bundled packages), business differentiator for keeping ahead of their competitor/rival illegal operation. Finally Customer retention; ensuring they can remain active to service their customer base at operator expense.

Therefore to be good at detecting and preventing fraud, operators need to think like the fraudster, think of all the elements of operator that can be defrauded, what information would they need to commit a fraud?, like sensitive company documents, internal processes and procedure documentation, sensitive account information, the access to sensitive equipment, employee personal data, finally fraudsters need to know details of fraud management controls and techniques.

### 2. 5. 2 Sources of Information (Robert and Dabija, 2009)

a. Operators need to consider where can the fraudster get this information?

b. How do they secure their information sources?

c. How easy is it to obtain this Information?

d. Would any compromise be detected?

e. How would it be reported?

f. How would it be escalated internally?

g. Who would investigate it?

h. What value does this information have externally?

i. How much damage could it cause?

### 2. 5. 3 Employee Compromise:

Employees are better placed than anyone to commit fraud, they are the key business asset and sometimes the main liability (Grant thornton, 2010), most employees are honest by nature, so operators need to keep them honest. Operators need to know:

a. What controls and restrictions do they enforce?

b. Are they vulnerable to blackmail, Peer Pressure and violence, these can have the desired effect?

c. Which are the employees with the most responsibility, are hey being controlled and watched?

### 2. 5. 4 Sale Channels:

Operators cannot operate without them but from a fraud perspective they need to be aware that, corrupt dealers and internal sales outlets do exist, they either operate alone or conspire with the fraudsters to commit fraud. They may "turn a blind eye to fraud" where the impact does not directly affect them and there is no operator deterrent, they still get paid, no claw back, contract termination etc.(agrawal.2010). Genuine dealers may be deceived by fraudsters, they trust the information being provided and they expect the Telco to approve what's presented, dealers are often the starting point for any fraud

### 2. 5. 5 Vendors: (Robert and Dabija, 2009)

a. Who are all the operator vendors?

b. What are they supplying to the operator and is it sensitive?

c. Have any vendor security audits taken place?

d. Has anyone visited their sites?

e. What information do they hold on the company?

f. What fraud protection and security arrangements have taken place?

g. Are these documented in the service level agreements and contracts?

h. Where does liability lie?

### 2. 5. 6 Media:

Articles, documentaries, news items etc… designed to highlight criminal activities can actually demonstrate how to commit a fraud. They have a detrimental and not a positive effect, fraud gets glamorized to some extent, the media portray that with telecoms there is no real victim, this is not true it is not a victimless crime. The media "highlight" an operators weaknesses, fraudsters perform "copy cut" crimes based on media information sources and it is increasing. (Robert and Dabija, 2009)

### 2. 5. 7 Internet:

Bulletin board systems (BBS) are regularly used by hackers and preachers. Often openly discuss ways in which to defraud telecoms, information needed to defraud anything from identity theft, credit cards, phone locking etc freely debated. Extensive intelligence can be gained from the internet, and the operators need to know what information is there on the internet that may assist the fraudster? What information is on operator's intranet site that may assist the fraudsters with attacks? (Robert and Dabija, 2009)

### 2. 5. 8 New Generations of Networks:

Next Generation Networks involving Internet Protocol (IP) traffic more vulnerable than existing General System for Mobile Communication (GSM) networks, all too often hacking information is publicly available, there are several freeware programs used to intercept traffic. "Regular" Internet fraud is rapidly going to move into the telecom arena, and the widely understood programming language makes it easier for the fraudsters, this will result in operators needing to learn new fraud prevention and detection skills. Existing fraud analysis practices will need to be expanded and different skill sets required. VoIP doesn't require the specialized equipment of tradi1ional telephony, so there's very little barrier to entry. (Bihina Bella,Oliver, Ellof, 2005)

### 2. 5. 9 Customers:

Operator's customers can also reveal information about a weakness in the Direct Access Method (DAM), which spreads by word of mouth. Vulnerability may have been discovered by one customer and before operator knows it an epidemic has occurred like a virus. (Robert and Dabija, 2009)

### 2. 5. 10 Suppliers: (Robert and Dabija, 2009)

a. All operators need equipment.

b. Operators suppliers build, implement and service there equipment.

c. Weak supplier security means that we are buying potentially weak equipment.

d. Suppliers often require dial-in access.

e. Do operators explicitly trust their suppliers?

### 2. 5. 11 Competitors:

Praesidium, find that most in country operators talk to each other and exchange views. However, commercially they cannot trust each other and must not become complacent. (Robert and Dabija, 2009).

a. What information do operators hold on competitor's products or services?

b. Will they have the same information about ours?

c. How secure therefore is our information?

d. Do operators know what weaknesses they have, their fraud levels etc?

e. Is fraud management viewed as a competitive Issue?

### 2. 5. 12 Fraud Information Sharing:

There are a number of sources available:

a. GSM Fraud Forum.

b. Forum for International Irregular Network Access (FIINA).

c. European Telecommunications Standards Institute (ETSI).

d. Telecommunications UK Fraud Forum (TUFF – UK).

e. Communications Fraud Control Association (CFCA).

f. A TFRA - Australia.

## SECTION 6: HOW IS FRAUDESTERS PREPERATING THE FRAUD?

**2. 6. 1 Leading GSM Fraud Risks**

**2. 6. 2 Things Fraudsters Want to Know**

**2. 6. 3 Three Main Fraud Driven Types**

**2. 6. 4 People Driven Fraud**

**2. 6. 5 Product/Process Driven**

**2. 6. 6 Technology Driven frauds**

### 2. 6. 1 Leading GSM Fraud Risks:

a. The main revenue impacting fraud losses are predominantly concentrated around the following primary frauds (otero. 2005):

   i. Subscription/identity.

   ii. Call Selling.

   iii. nationally/ internationally.

   iv. Roaming.

   v. PRS/ Internal Revenue Service (IRS).

   vi. By Pass.

   vii. Internal.

b. Other secondary fraud losses will derive from either the product and service offerings or the way in which operator actually choose to sell their services:

   i. Dealer/Sales Channels.

   ii. Prepaid.

   iii. Payment.

### 2. 6. 2 Things Fraudsters Want to Know: **(Robert and Dabija, 2009).**

a. What proofs of identity are required?

b. How is the customer information going to be validated?

c. Is a credit vetting procedure carried out?

d. What services are immediately obtainable?

e. Will I need to pay any form of deposit or security for service?

f. When will the first bill be mailed?

g. Will I be able to obtain multiple SIMs?

h. What handsets are being promoted?

i. Where does the first invoice go to?

j. Will excessive usage lead to a customer services call?

k. How long can payment are delayed?

l. Will part payment ensure continued service?

m. If payment is cash, can a credit check be avoided?

## 2. 6. 3 Three Main Fraud Driven Types:

**- People Driven:**

a. Using people inside the organization to perpetrate the fraud

b. Using organized crime syndicates outside the organization to perpetrate the fraud

**- Product/Process Driven:**

Using/abusing special characteristics of operator products/processes to facilitate the fraud

**- Technology Driven:**

a. Attacking operators materials/machines to perpetrate the fraud

b. Using tools to commit fraud

## 2. 6. 4 People Driven fraud:

Fraudsters looking to exploit the person and preying on an Operator's vulnerabilities

### *2. 6. 4. 1 Social Engineering:*

Social engineering and the exploitation of people is the fraudsters' biggest weapon. It means that a fraudster can try all sorts of ways in which to 'get information or manipulate people to commit fraud, it is also a way of pressuring operators to do something that they shouldn't or don't want to do. It is easy to obtain information if one has a valid pretext and, in addition, offers some sort of "reward". Significant social engineering campaigns are spreading across Eastern European operators currently, customers were targeted with SMS campaigns announcing they had won a prize and they should call a specific number. Once they called, the fraudsters presented themselves as operator representatives" advising the customer to buy prepaid vouchers and tell them the Hidden Recharge Number (HRNs )in order to pay for the "taxes and transportation" – this is simple, and in many cases effective. (Allen, 2010)

### *2. 6. 4. 2 Pre Texting*: (Schneier, 2009)

a. Pre texting is the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is usually done over the telephone

b. It's more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information (e. g. , for impersonation: date of birth, Social Security Number, last bill amount) to establish legitimacy in the mind of the target.

c. This technique is often used to trick a business into disclosing customer or sensitive information, and is also used by private investigators to obtain telephone records, utility records, banking records and other information directly from junior company service representatives.

### *2. 6. 4. 3 Dealer Fraud:*

Dishonest dealer's operators highlighted under channels and they can and do cause substantial losses from (B/OSS, 2007):

a. Subsidy Abuse.

b. Equipment.

c. Commissions.

d. Ignoring or violating pre and post validation checks.

e. Collaboration with the fraudsters.

f. Black Marketeering.

g. Promotions Frauds.

h. Advertising Frauds.

### 2. 6. 4. 4 Identity Theft:

One of the fastest growing crimes in certain countries, not just related to telco's but all types of financial service. Fraudsters may assume the identity of another "genuine person" in order to obtain service, they can also create identities which are even harder to detect once established, generally fraudsters are using details that are guaranteed to pass credit checks, customer profiling and validation, they will obtain information from any source computer records, paper records, (steal it, pay for it, simply just find it!). It is often the case that fraudulent accounts will initially look like and behave like operator best customer, in certain countries they pay people to "use" their identities to obtain telecom services (otero. 2005)

### 2. 6. 4. 5 Subscription Fraud:

Probably the primary and most widespread fraud type being experienced today, and wherever there is postpaid service there is no exceptional, it takes advantage of loopholes and procedural weaknesses in customer take on and validation. Predominantly involves the use of forged papers, fake documents or the use of genuine papers by a different person other than the legitimate owner, it can be performed as an individual attack or as part of an organized subscription fraud ring, it is looking to maximize the number of fraudulent accounts/SIMs. Subscription fraud constitutes the basis for more damaging fraud types, such as Roaming or PRS fraud, in a lot of instances will be linked directly with other secondary frauds, e. g. dealer fraud. Increased innovation for products and services fuels more subscription fraud therefore it will increase. Organized subscription fraud creates bad public relation and genuine customers lose the trust and faith in an operator (otero. 2005 )

### 2. 6. 4. 6 Controlling the Risk of Subscription Fraud:

a. The ability to actually protect against fraud is heavily dependent on the overall attitude of the operator, do they provide postpaid to all customer segments-residential (1-3 SIMs), business SME (1-20 SIMS), Corporate (Limitless).

b. Is there specific classification criteria in place as to what constitutes each type of customer, these practices vary considerably from operator to operator?

c. Are the sales channels incentivized and encouraged to be "fraud free" or to "turn a blind eye".

d. Are front end processes robust and adhered to, that means is there documentation accuracy, information validation and customer verification practices.

e. What input is there from the Fraud Team regarding prevention, and finally how are losses associated to subscription fraud measured and reported (agrawal.2010).

### *2. 6. 4. 7 Extending the Fraud – Paper Company/Long Firm Fraud:*

Organized fraudsters will masquerade as a genuine company, initially will continue to operate as a normal (first 90 days) in order to obtain additional services/capacity, they Will ensure they have a good payment history 50 account credit limits will be raised, they also will operate from furnished offices that have been rented to appear as genuine company. As traffic consumption increases they will begin to challenge the billing but still request additional capacity/SIMs, whilst disputed billing amounts are being challenged they will have already created the next, paper company" and obtained service. In essence they are simply bogus/false companies requesting service and exploiting weak sales processes. (Robert and Dabija, 2009).

### *2. 6. 4. 8 Extending the Fraud – Bill Spreading:*

Bill spreading enables the fraudster to have multiple accounts across different bill cycles (where this practice is allowed). The fraudster will look to maximize the number of accounts and time periods, they looking contractually that each account is treated as an "individual account" and therefore none payment on one account does not affect the others, no suspension of service. Operators are in fact providing the fraudster with continued service to operate his business whilst he accumulates further debt unless the linked accounts can be identified the fraud will not stop, as the attacks are now in another bill cycle and will only possibly be detected during the collection cycle and treated differently. (Robert and Dabija, 2009)

### *2. 6. 4. 9 Extending the Fraud – Address Changing*

This is a common technique employed by fraudsters, fraudsters will use a genuine address at first in order to pass any customer validation or credit checks, immediately service is approved they contact customer services to advice of a change of address, the second address is not subject to any form of checking and the account details are simply changed.

These changes are made before any bills or correspondence (welcome letter) is posted, so as to avoid detection. The person at the genuine address is unlikely to receive any correspondence from the operator. (Robert and Dabija, 2009)

### *2. 6. 4. 10 Payment Fraud Types*: (AFP, 2007)

a. Stolen checks:

    i. Checks fraud has existed since checks were first introduced.

    ii. Instances of checks fraud have reduced considerably.

b. Altered or forged checks:

    i. BT and other Telco names are vulnerable.

    ii. Company/business accounts (ceased trading/bankrupt).

    iii. Credit cards - 8tolen or fake (cloned) cards.

c. Bank transfer (direct debit) fraud:

    i. Using genuine person's details.

    ii. "hiiacking" the direct debit mandate.

#### a. Credit Card Fraud:

Global figures on losses increasing annually and seen as one of the fastest growing crime internationally (Confidence group, 2004). Overall credit card losses estimated to double in next 5 years up to $15. 5 billion, so Telco's will be targeted ( Confidence group, 2004). UK losses alone estimated at $3billion. Current financial crises increase the amount of credit card fraud, Credit card fraud is one of the simplest types of fraud to commit, no technical knowledge required and internationally prevalent. Operators need to pro actively limit the exposure as it is almost impossible to eliminate this threat.

a. Types of attack will come from one of these(Grandhi, 2010):

    i. Theft of credit cards.

    ii. Identity theft.

    iii. Compromised card details.

    iv. Card Not Present.

    v. Counterfeit cards.

    vi. Number generation software.

    vii. Carding. . . . . Testing and validating a card over the web.

b. Detection is normally via transaction declines. Complaints or charge backs but in a number of cases identified far too late.

### *2. 6. 4. 11 Providing Tools and Information fraud:*

a. Fraudsters profit from creating tools to commit fraud or selling information.

    i. Selling Prepaid Hidden Recharge Numbers (HRNs) or Personal identity Numbers (PINs) for Calling Cards

    ii. Selling handset unlocking codes

    iii. Selling handset unlocking software

    iv. Cloning equipment/magic phones/scanners etc

b. In certain countries they are safeguarded against prosecution as they do not actually commit the fraud or there is no defined legislation in place.

### *2. 6. 4. 12 Unauthorized Bonuses or Account Credits fraud (internal fraud):*

For prepaid accounts operators apply different airtime bonuses to accounts via different methods. Employees are generally allowed to apply customer credits for billing queries or mistakes. Operators sometimes assign different levels of crediting against different grades of employee. However, in a number of instances, multiple bonuses or credits can be applied to "friends and family" month in month out. What protection is in place to ensure that unauthorized credits are not applied to customer accounts on both postpaid and prepaid services (Kurtz, 2002).

for example African operator billing manager responsible for performing airtime bonuses to prepaid accounts, no one else really had the system knowledge. Identified a fraudulent method of provisioning credits to certain accounts. Once the transaction was performed he had the ability to remove the details and as long as airtime quickly consumed then no audit trail .System audit logs were also "deleted" for a 3 month period. Investigation resulted in employee dismissal, changes to prepaid system security and the application of bonuses.

### *2. 6. 4. 13 Physical Security Compromise Fraud:*

Weak physical security will enable fraudsters to commit a number of attacks relating to:

Equipment theft, theft of commercially sensitive information, unauthorized access to systems physical attack on key network elements (Base stations, MSCs, exchanges), and theft of personal belongings. What access controls and restrictions do operators have in place to prevent this?

## 2. 6. 5 Product/Process Driven:

Using/abusing special characteristics of operator products/processes to facilitate the fraud

### *2. 6. 5. 1 Call Features Abuse:*

A fraudster will look to use value added services and call features to magnify the effect of the fraudulent attack. Most common features used in fraud are Call Forward and Call Conference - usually in conjunction with either Roaming or Premium Rate fraud (or a combination). But do operators allow unlimited call forwards? Do they monitor for any suspicious calls that use these features? do they know of any genuine instances of conference calling when roaming? (Brown, 2005).

### 2. 6. 5. 2 Call Forward Fraud:

Similar to conference calls in that the feature allows the real caller to be hidden. In Direct In-System Access (DISA) frauds, call forwards set on regular basis allowing through calls to be made (Brown, 2005).

### 2. 6. 5. 3 Conference Calling Fraud:

Identity of real fraudsters and to maximize the value of PRS fraud, it allows multiple connections (chaining) of calls. Means for perpetration of call selling, it is used in DISA frauds to act as a call operator in the same way as a switchboard. (Brown, 2005)

### 2. 6. 5. 4 GSM Call Selling:

As advised previously SIM cards are obtained using fraudulent papers or by paying genuine customers to provide their details, the fraudsters "service" is advertised usually over the Internet, in local cafes, or call selling cabins, calls (IDD) are sold at highly discounted prices. The most effective fraudsters use Call Forwarding feature to maximize the profit, as there are unlimited simultaneous calls that can be made. It's very hard to detect without an FMS because usually the SIM is used just during one night, discarded and then another SIM is used. Depending on the knowledge of the fraudster, the operation can vary from a one shot fraud, to a whole business, involving sellers, operators, etc.(LIoyd,2003)

A "Call Selling" example: Customer applies for a number of SIM cards for a local business, very low or no traffic is made during the first few weeks, even a month (no traffic should have been a fraud indicator!). High volume of traffic was then made from the same location, usually during the night or weekend days. The Operator realized the calling activity was not in line with the business activity, customer was subsequently suspended but the damage was already done. The account activation papers used turned out to be forged, and the customer was uncontestable on the other numbers provided and the real person claimed he had no knowledge of the subscription!

- **Premium Rate Services Fraud:**

Mostly used in conjunction with other fraud types. The main motives are to make free calls to high cost numbers like competition or hot lines, and also to make money from falsely generating calls to a number owned and operated by the fraudster. The more calls generated, the higher the profit to be made (Hoath, 2008).

PRS Fraud Currently probably considered the most financially damaging fraud type in combination with Roaming. Fraudsters are normally looking for smaller. Un- prepared operators. This fraud type is trans-national, so borders have no relevance. In well organized attacks the calls are made during weekends, holidays, etc in order to take advantage of a bigger time-window, until the first Roaming High usage report HUR is received. (Robert and Dabija, 2009)

### *2. 6. 5. 5 Roaming Fraud:*

The roaming fraud principle is that the home network is responsible for its customers (and their cellular identities) when roaming on another network, irrespective of the fraud type. The visited network will only be liable if the roaming agreement has not been complied with Call Details Records – CDR's or fraud alerts not sent on time. (Doe,2008)

Abuse of roaming facilities to make free calls has been a major issue for a number of 0perators with reported losses being in millions. Roaming subscription fraud has been the major problem across the GSM world (SIM card is simply taken to another market). Also roaming PRS now becoming the most damaging fraud type. But does the visited network really care as long as they abide by the "rules', they make money as well. Satellite roaming problems also occur in the delivery of information. Also prepaid roaming fraud increases as operators are not prepared for it, and sometimes not even looking at prepaid Test Access Path (TAP) files (doe, 2008).

### *2. 6. 5. 5. 1 Cost of Roaming Fraud:*

Losses due to roaming fraud are now estimated by some to be 50% of overall fraud loss, a 25% increase over the last 2 years. Annual roaming fraud losses exceed USD 3. 5 billion, according to Communication Fraud Control Association (Robert and Dabija, 2009). GSM Fraud Forum FF regularly reports roaming fraud as being the second highest fraudulent attack for operators globally.

Preventive measures to fight this type of fraud are therefore an important priority in fraud management initiatives Near Real Time Roaming Data Exchange (NRTRDE). Operators must not look at Service Difficulty Reports (SDR) value alone on a high usage reports (HUR.) Another important issued to be highlighted is roaming fraud is a lucrative business; fraudsters will pay deposits if necessary in order to obtain service, so operators must learn the lesson from others costly mistakes. (Doe, 2008).

### ***2. 6. 5. 6 GSM Cloning:*** (Brookson, 2005)

a. What actually is GSM cloning:

   i. Get the International Mobile Subscriber identity (IMSI) of the SIM.

   ii. Get the Ki (individual subscriber authentication key).

   iii. Write them on a. smart card (also known as gold/silver card).

b. Cloning has been occurring since GSM started:

   i. Manufacturer errors.

   ii. Twin SIMs.

c. COMP128 v.1 (algorithm which is used in GSM network for authentication purpose) authentication algorithm compromised - Operators still use this due to business cost of replacement.

d. Cloning requires presence of SIM card (not over the air), access to the PIN code and just a couple of minutes alone with a PC.

e. Introduction of COMP 128 v. 2 has decreased the level of risk of cloning, but many operators still use COMP 128 v. 1, and also older SIM cards are still COMP 128 v.1, so the threat is still real.

f. Previously cloning was a bit of science fiction, requiring good technical knowledge, and considerable processing power currently, pre-programmed SIM emulation cards are used.

g. Up to 8 IMSIs and KI can be on the same card.

h. IMSI and individual subscriber authentication Key are registered via the menu option,

i. Sold as a package.

j. SIM Scan free to download from the Internet.

k. Cheap Card reader tools as SIM Master, Maki or Phoenix (Telecom Solutions) interface are used, very easy to procure.

### 2. 6. 5. 7 Bypass:

Sometimes being referred to (wrongly) as "VoIP fraud". But VoIP is not a fraud type. The purpose of bypassing is making money by illegally terminating traffic (usually international traffic) into operator's network, without paying the interconnection fee, using VoIP technology.

Fraudster usually is a business with high turnover. They has contract with a wholesale operator for a determined number of minutes to be terminated via his SIM cards. Traffic is being received via IP and is routed through the fraudster's, SM gateways (SIM boxes), it reaches the destination as a national call. The fraudster will pay the network for a national call but will charge the Wholesale operator for every minute he terminated; the Network Operator loses the Interconnection fee. (Cohen and Southwood, 2004)

### 2. 6. 5. 8 SIM Boxes:

Different kinds of equipment that can accommodate a number of SIM cards. They have connection to Internet. Some of them have external GSM antennas. It can be used for legitimate traffic as well, such as a business' external traffic. Their main function is to transmit traffic to its destination .(Sevis systems)

### 2. 6. 5. 9 Interconnect Re-origination:

The origination number of the call is replaced by a local number by the sending operator allowing the call to be priced without the route based pricing method. Mainly used where the interconnect International Telecommunication Union ( ITU) pricing method is in place as this uses a mixture of the A number, B number, and actual routes used to derive the price (Davey, 2009).

### 2. 6. 5. 10 Prepaid Fraud:

Prepaid viewed by many as being so simple to operate. Don't even consider or look for fraud risks. Many prepaid frauds associated with 'technical Issues' - initially viewed as revenue assurance problems but soon become targeted by fraudsters, some of the larger frauds are inextricably linked to internal illegal activity. Often no one accepts overall responsibility for prepaid fraud management, it's fragmented. There is no direct ownership of the various elements of the service or products, no defined fraud strategy. In prepaid services there is lack of documented flow processes exist with built in protections, that means no end to end protection, also inadequate monitoring and reporting; poor visibility across the service (javeline strategy and research ,2009)

### *2. 6. 5. 10. 1 Prepaid Fraud Attacks:*

Prepaid vouchers are essentially money, but are not treated the same by most of the operators, they should be handled and managed as though they were "cash". HRN generation and supporting processes are weak and lack fraud controls or security. Also voucher design; production and printing are left to the vendor to determine, and this is bad practice. Voucher logistics and transportation are not planned and exposed to the risk of a concerted theft, another issue is voucher warehousing and storage is generally weak. All these are extremely high risk areas, with high potential for fraud (javeline strategy and research, 2009).

### *2. 6. 5. 11 Top Up Fraud – 3rd Party Compromise:*

Major Caribbean Group operator, offered Vendors direct connection to the intelligent network, in order to provide retail top ups to customers. "Credit purchased in advance at wholesale rates and connection through **virtual private network**( VPN )for credit management. AII credit purchased by the Vendors held in a single bucket. One Vendors equipment located on operating countries OPCOs premises, even though the OPCO had no access. there is no specific rules in place regarding maximum account balance or transfer rates. Rogue Vendor employee used credentials to access the wholesale account and started transferring large amounts of credit to multiple SIM cards - distributing the fraud attack. (Robert and Dabija, 2009)

### *2. 6. 5. 12 GPRS Overbilling:*

Attacker initiates session to a malicious server, server starts sending data, the attacker then disconnects and the server continues sending data. Legitimate users connect and gets assigned attacker IP, they will get the data sent by the malicious server which will result in significant invoice inflation. Also resulting in bad public relation and likely that the operator will have to compensate for the costs. (Bavosa, 2004)

### *2. 6. 5. 13 Calling Card Fraud:*

This has ranged from the use of modified cards, to the stealing of card numbers and PINs, it is very easy to perpetrate since many operators do not check usage on calling cards. Classic example involves calls being placed to public phones that have their rings turned off, when the victim picks the phone up, a fake dial tone is transmitted, card number are register as Dual Tone Multi Frequency (DTMF) tones and then translated into digits. The call is released and the victim has no idea he has just been defrauded. (Bavosa, 2004)

### *2. 6. 5. 14 Shoulder Surfing:*

The technique used by a fraudster to obtain information such as account numbers and PINs, not only in Telecoms, but also in banking industry. In simple terms, one watches over your shoulder and remembers the digits you pressed on the phone or A TM machine more sophisticated fraud involves the use of high fidelity video equipment to monitor the PINs entered by the customer, normally at airports etc.(Kumar,grinfinkel,bonen and winograd)

## 2. 6. 6 Technology Driven Fraud:

### *2. 6. 6. 1 SS7 Manipulation Fraud:*

Several SMS services on the Internet offering "free" SMS, have operator ever considered that they might be doing it at their expense?

Fraudsters use modified platform to send altered 'Signaling System SS7 Messages. If uncontrolled, the SS7Network will take these messages and route them as if they were made by operators own subscribers. In most cases, fraudsters use bogus Mobile Subscriber ISDN Number (MSISDN) ranges so that the fraud is not discovered by means of customer complaints. Still, the operator has to pay the price for terminating SMS on other networks (Rey).

### *2. 6. 6. 2 Blue jacking Fraud:*

IT not related to any form of hijacking, it is the transmission of unsolicited images or text via a Bluetooth link, to a targeted phone, laptop or Personal Digital assistant (PDA), The target needs to be in "Discoverable" mode. Many users still not aware of security risks with Bluetooth so they don't check Bluetooth status. It is relatively harmless, no real damage is done but it can be used as a means to propagate offensive messages, threats, etc.(c ck,2008)

### *2. 6. 6. 3 Bluesnarfing Fraud:*

Bluesnarfing fraud is depending on phone model, the attacker has access to several features (cck, 2008):

a. Accessing SMS history.

b. Sending SMS.

c. Accessing Contacts.

d. Accessing Calendar.

e. Making Calls.

f. Creating Call Diverts.

Information on know how publicly available on the Internet. There are several software tools already available, for both Blue jacking and Bluesnarfing:

a. http://www. blujackingtools. com

b. http://www. bluejackg. com

### *2. 6. 6. 4 DISA/PBX Fraud:*

Customer equipment is vulnerable to attack; it nnown as Direct Inward System Access (DISA) fraud. Risk increases due to a lack of understanding of risks by the customer, they "trust" or rely on the PBX provider to provide the required security settings to prevent fraud. Recent victims have included Telecom Operators, financial institutions, anyone who is normally involved in making high numbers of IDD calls. Remember it will not be the Telecom provider that is defrauded; it will be the customer whose PBX is abused who suffers the loss.(cck, 2008)

### *2. 6. 6. 5 VOIP Risks:*

A VoIP caller can be anywhere and can easily use unauthorized billing information or credit card details, classic scams such as personal information theft could increase as there is no longer a location for an end point. Even IP source and destination screening does not really help. A call may 'terminate' in another country, creating a new set of consumer rights and legal issues. Even though the technology exists, the tracing of IP call routes has not been well-planned or executed to date and Peer to peer type technology is dynamic (Doten,2008).

### *2. 6. 6. 6 IMEI Duplication*:

IMEI (International Mobile Equipment Identity). Integrity of IMEI has been compromised in a number of manufacturer's phones, continually being targeted despite the security levels adopted. Fraudsters able to avoid blacklist detection with thousands of handsets being programmed with the same IMEI. Operators obviously reluctant to bar handsets with the same IMEI numbers as 'Legitimate' customers will also be cut off. In certain countries due to the level of handset theft Operators being forced by the government to use .The IMEI s used in conjunction with other techniques, for example. Cloning. It is also Linked to other forms of criminality. (Celtel, 2006)

### *2. 6. 6. 7 Phone Theft:*

Mobile phone theft has risen 190% in recent years. In the UK a handset is stolen every 12 seconds; phone jacking is costing UK consumers $M780 every year. Fraudsters now developing increasingly sophisticated techniques to pass off stolen handsets as legitimate.

Evidence of new techniques being developed to conceal stolen phones has been uncovered where the UK Police suspect crooks are taking stolen handsets, illegally changing their IMEI numbers and then giving them fake interiors complete with counterfeit IMEl labels own 'production plants. Incidents of mobile phone theft /Snatching are also on the rise worldwide, cases involving mobile phone thefts top the list of crimes reported in Bangalore. (Robert and Dabija, 2009)

### *2. 6. 6. 8 SMS Inflation:*

SMS chat line services joined by completing registration SMS to provider, that resulting in SMS from other members which were paid for by recipient. The prices varied between $0.7 and $4 per message. Some providers set limits on number of SMS that could be received before re-registering was required. Customer needed to issue SMS to end the chat, they were being bombarded with SMS and suffered high bills which resulted in bad debt/ fraud, estimated loss $22, 500 per month (ISCE, 2010)

### *2. 6. 6. 9 Mailbox/Voicemail Fraud:*

Voicemail/mailbox call back' feature (Northwestel):

a. Has been abused if mailbox can be accessed from landline or mobile with no pin codes or a number verification of mailbox owner.

b. Voicemail is also abused on networks that use a "default PIN for access, especially if International calls can be made; Message can be left from number which is then diverted to international destination. Call made back to mailbox and 'call back' used to dial phone number which is on divert.

### *2. 6. 6. 10 Ghosting:* (Doten, 2008)

a. Normally associated to internal system or equipment abuse, it means applying services directly into the switch without amending the billing system.

b. Re-activation of used prepaid HRNs.

c. The removal of records from the billing system.

d. Removal/changing of flags and settings of customer accounts.

e. Creation of fictitious accounts, customers or employees.

### *2. 6. 6. 11 Box Splitting:*

The term used for breaking down mobile handsets and equipment to be used or sold separately, sometimes handsets appear on the grey market and sold globally. Box splitting can increase the losses of a fraudulent attack, and can also disperse the fraud over a large geographic area. It is extremely popular where subsidized markets exist where operators experience huge handset losses. Later identifying that equipment has been re branded and openly on sale in neighboring countries. Box splitting sometimes impacts on the actual manufacturer as "inferior" products are being sold as the genuine article (Doten, 2008)**.**

## SECTION 7: DETECTION AND PREVENTION

**2. 7. 1 Basic Principle and Requirements**

**2. 7. 2 Recommendations about WhereLoopholes Exist and How they should be Minimized or Closed**

**2. 7. 3 Prevention and Detection – Prepaid Techniques**

**2. 7. 4 Blacklists/ Hotlist Management**

**2. 7. 5 Case Management**

**2. 7. 6 Reporting and Measurement**

**2. 7. 7 Why do Operators Need Fraud Categorization and Reporting**

**2. 7. 8 Detection Approach – Fraud Risk Assessment**

**2. 7. 9 Best Practice Fraud KPIs - Postpaid**

**2. 7. 10 Prevention Measures**

**2. 7. 11 Focus on Loss Prevention**

**2. 7. 12 Fraud Risk with New Product and Services**

**2. 7. 13 Evaluating New Products and Services**

**2. 7. 14 Effective Measures – Detect and Protect**

**2. 7. 15 Fraud Management Methodology in Developing Countries**

### 2. 7. 1 Basic Principles and Requirements:

To detect fraud operators need to have or act upon the following (Roberts, Dabija. 2009):

a. The operator therefore needs to have a fraud management structure that ensures that they focus on the greatest potential financial loss due to dishonesty.

b. The operator need to have a structure in place to ultimately limit the total exposure to fraud across the business and not isolated to customer airtime loss.

c. The operator need to have a clear idea of what fraud management costs, fraud losses and a formula to calculate savings and recoveries.

d. Operator need to be actively protecting their customers as well as their own network.

e. Operator need to be progressive and forward thinking in there approach to detecting, investigating, controlling and ultimately preventing fraud.

**Operator Fraud Team Needs to Understand:**

a. What is actually being targeted and by who, what are the operator up against?

b. Understand the local culture and demography, where is the operator most vulnerable or exposed.

c. Determine the existing skills and expertise, do the operator have the correct skill sets and resources.

d. Take into account any legal/regulatory legislation constraints over providing service, do operator know what they can and cannot do to prevent fraud.

e. Appreciate the types of product or service provided.

f. Be aware of local or internationally organized crime groups, who is operator taking on?

g. What information sources are currently available to assist in fraud monitoring, detection and prevention?

h. What are the common fraud indicators that operator are using to trigger alerts, reports of illegal activity?

i. Have the operator been able to establish clear lines of communication throughout the business?

j. Development of reporting capabilities. What is in place?

k. Procedural enhancements. Who owns them and ensures compliance?

l. Education and awareness, what program is in place internally?

**There are Some (KFIs) in Preventing and Detecting Fraud Should be Mentioned, but are not Limited to:**

a. Undelivered invoices mail.

b. Returned/declined payments.

c. Un-contactable customers.

d. Changes in address information immediately after registration.

e. Roaming with little or no home network usage.

f. International calls.

g. high usage - multiple IMEIs used.

h. Multiple accounts/SIMs.

### 2 .7. 2 Recommendations about Where Loopholes Exist and How they Should be Minimized or Closed: (Roberts, Dabija. 2009)

#### *2. 7. 2 .1 Fraud vs. Bad Debt (Receivables) Separation:*

The eventual ability to write off non receivables (bad debt) is an option for all operators but fraud should never be written off without formal investigation. Fraudsters will always seek to reacquire service and each time they apply, they have additional information on how to exploit weaknesses in the company's systems, procedures, and processes. Identifying fraud early will reduce the demands on the credit control and collections departments and save effort and money that may be required to seek legal follow-up of an account, which is a time consuming process. By leaving the cost of fraud in the bad debt figure, it is not possible to identify the extent of fraud or determine whether fraud is being adequately controlled or whether the levels are increasing month by month.

It is also not possible currently to determine whether a particular product or service is being targeted if there is no actual separation of uncollected debt by product or service type. Once fraud is identified, the methodology used that enabled the fraudster to obtain an account can be reviewed to allow earlier identification methods to be determined. (GOLIAT, 2004)

### *2. 7. 2. 2 Call Detail Analysis:*

An essential part of any fraud investigation involves analysis of call details made on a fraudulently used SIM/phone. On a fraudulently acquired account where everything on the application form is considered false, analysis of call records is critical in determining any linked accounts and possible organized fraud, resulting in call selling operations, roaming or international premium rate fraud which would be considered high risk exposure for the business. Most proactive telecoms fraud functions are now using analytical software tools such as Choice point's 12 Analyst Notebook, Watson or Pen links which have the ability to import thousands of records, either call data, or name address data etc, and automatically find the links between individuals, groups and premises, a process which would take an enormous amount of time if done manually. These software applications allow the Fraud Analyst to (Bihina Bella, Oliver, Ellof, 2005):

a. Demonstrate clear links between fraudulent accounts showing the common numbers dialed by the suspect fraudsters.

b. Show clear links between other subscribers calling records and a known fraudulent account - e. g. roaming and PRS fraud.

c. Identifies hot/control numbers to add to an FMS or into a Blacklist.

### *2. 7. 2. 3 Roaming Fraud Management:* (doe, 2008)

a. Set business rules for providing and restricting roaming services - number of SIMs, customer classification etc.

b. Determine and set realistic investigation thresholds for cases per day by value etc that avoids duplication of effort.

c. Practices should include reviewing the account's usage, bills paid and method, existing calling patterns, unbilled airtime, number of SIMs etc.

d. Track known fraud instances - build fraud intelligence database (IMEls, Called numbers, destinations, high risk operators, etc).

e. Provide roaming fraud awareness training to "front line" employees - ensure there is free flow of information across the business.

### *2. 7. 2. 4 Applying Roaming Restrictions:* (doe, 2008)

Many networks restrict the following services:

a. Call Forwards.

b. Call Waiting.

c. Multi Party.

d. Barring - incoming when roaming.

e. Barring - outgoing except to home Public Land Mobile Network (PLMN).

f. Explicit Call Transfer.

g. Operator Determined Barring.

h. Premium Rate.

### 2. 7. 3 Prevention and Detection – Prepaid Techniques: (Roberts, Dabija. 2009)

a. Required to define an actual strategy for managing risks.

b. Ensuring ownership and accountability of risks.

c. Vendor and supplier liaison, defining the standards/contracts.

d. Monitoring of activities, system user access, bulk loading of credits, manual adjustments etc.

e. Reconciliation of account balances - reporting and visibility

f. Alerts on IN flags - FMS where possible.

g. Continuous "monitoring and testing" of different scenarios - what if!

h. Customer complaint evaluation.

i. Continuous voucher testing practices.

j. Activation timings enforced across all systems.

k. Incident reporting centrally controlled

l. Periodically evaluate the controls and protections in place.

m. Ensure system based logs are being reviewed.

n. Establish effective reporting methods for potential security breaches and fraud.

o. Product and service design - build in security and fraud protection at all stages.

p. Adopt jigsaw approach on sensitive data - four eyes principle.

q. Open up lines of communication across the business.

r. Exchange information with other operators. Develop "a training program for staff in the basic awareness of fraud and security risk

### 2. 7. 4 Blacklist/ Hotlist Management: (Roberts, Dabija. 2009)

a. Following the detection of fraud, distinguishing characteristics of the case should be populated into a blacklist/hotlist for reference when new potential fraud cases occur.

b. Criteria such as hot B numbers, cell sites, names, addresses, IMEI, countries etc can be populated into the FMS to enable rapid type alarms to be generated once a subscriber matches hot listed data.

c. Many operators implement a blacklist of known fraudulent details within the network and link this to the activation process to prevent new applications from being activated using known fraudulent details.

### 2. 7. 5 Case Management: (Cortesao, Martins, Rosa and Carlho)

a. All fraud cases should be recorded in order to utilize the information for intelligence purposes and to enable proactive detection of fraud in the future where fraudsters use similar names, ID numbers, addresses and calling profiles.

b. The recording of cases will also enable fraud losses to be recorded to facilitate financial reporting to management and CFO on losses. This can be achieved by recording all cases in the FMS, if operators have implemented one. (changing from the manual recording practices).

c. Each fraud case when identified should have a file created with an index containing the case reference number; the MSISDN, name, address, fraud type/source and some remarks to assist the fraud team to understand what each case is about. .

d. A brief final written report should be completed detailing any corrective actions taken by the fraud team or identifying areas within the business where exposure was identified.

e. Feedback must be received as to whether the recommendations were auctioned or not and only then should a case be closed.

f. Advice should always be sought from legal in respect of retaining evidence for fraud case prosecution.

### 2. 7. 6 Reporting and Measurement: (Shelton, 2003)

a. The fraud team will still be responsible for providing senior management with reports and will be required to accurately measure fraudulent activity within the business.

b. To facilitate this, the fraud team should maintain and manage various daily and monthly statistics, which will be used by the fraud manager to accurately measure fraud trends and losses.

c. Predominantly the fraud team will be responsible for the quantification of fraud losses, (e. g. average fraud per case, average roaming fraud loss per case, hot destinations (nationally/internationally), and frauds per product / service type etc.) The fraud trends reporting should be categorized into the different types of fraud detected and their source (e. g. subscription, call selling, roaming, account credits (prepaid), payment fraud etc)

### 2. 7. 7 Why do Operators Need Fraud Categorization and Reporting (Shelton,2003)

a. It is unlikely that a problem will be corrected if no one knows the problem exists.

b. The reactive approaches of the past used for fraud loss detection often led to significant delays in the detection of problems -Increased exposure, e. g. roaming fraud/HUR delays.

c. Proactive identification of fraud leakage and reducing delays enables rapid response and correction, reducing losses through early intervention, needs fraud team to be mandated to act accordingly when faced with a risk, not to need approval for account suspension/termination.

d. Requires access to all areas of the business, all data sources, personnel. Information.

e. Identification of KPls for the fraud team should be determined by the business.

### 2. 7. 8 Detection Approach – Fraud Risk Assessment (Estevez,held and peze,2005)

a. Interview line managers - what are the perceived problems, weaknesses, opportunities for fraud in their areas.

b. Interview the "workers" - what is the reality, stumbling blocks.

c. Obtaining supporting data - network, billing, finance existing reporting and reconciliation.

d. System Integrity - defining security and ownership.

e. Escalation practices and incident reporting

f. Analysis and categorization - quick wins, medium term and longer term.

g. Follow up - action plan, allocated on basis of time, benefits and activity required.

### 2. 7. 9 Best Practice Fraud KPIs – Postpaid: (Smith, 1998)

a. Frauds Identified , means classification required (subscription, IDD, roaming, PRS, By pass etc).

b. Number of "attempted applications' declined.

c. Average fraud value/loss per account/MSISDN

d. Fraud value split by reason.

e. Fraud value split by customer segment.

f. True cost of fraud trending (True Cost of Fraud has to include apart from visible losses, the Network Cost, Interconnection cost, Subscriber Acquisition costs, Commissions, Equipment subsidy, etc).

g. Fraud value' split by geographical area.

h. Fraud value split by sales channel - own shops, dealers, indirect telesales etc reported fraud losses as a % (taking into account % of bad debt).

i. Speed of detection in days/run rate - average number of days an account was active on network.

j. Source of detection - FMS, Customer Complaint, Informer, Welcome Call etc.

k. Total fraud loss – weekly/monthly/quarterly.

l. Fraud analyst cancels per day/monthly - FMS targets.

m. Fraud analyst reconnection rate - measuring the fraud detection process.

### 2. 7. 10 Prevention Measures: (Smith, 1998)

a. The Fraud Team can use a number of techniques and tools in order to effectively detect, analyze, monitor, prevent and report on fraud.

b. All fraudulent attacks identified should be used to prevent future frauds if the fraud team are to reduce the company's exposure.

c. It is preferable that system controls are used instead of procedural controls in order to prevent abuse of service.

d. Analysis and identification of the techniques used and an understanding of the methodology will allow the fraud manager to determine the most effective prevention strategy to be deployed.

e. There must be an understanding as to the commercial implications to the business when developing preventative measures.

f. There are a number of different prevention measures:

    i. Policy related.

    ii. Process and procedural related.

    iii. Person related.

    iv. IT system related.

    v. Network system related.

    vi. Physical security related.

    vii. Combinations of the above.

### 2. 7. 11 Focus on Loss Prevention:

As greater confidence is gained in detection ability, operators must move towards increased focus on prevention. This needs to focus on the following (smith, 1998):

a. Involvement in the product and services development cycle - assessing the risk.

b. Root cause analysis - determining the problem, gaps or inherent weaknesses and defining the required controls.

c. Evaluation of existing processes for loss exposures - is the risk technical, procedural or people based?

d. Uncover - identify and investigate potential issues.

e. Discover - analyze, quantify and qualify issues identified.

f. Recover - implement corrective initiatives to resolve issues.

g. "Prevention is better than detection".

### 2. 7. 12 Fraud Risk with New Product and Services (elemen customer care, 2008)

a. Each product and service in the market represents a potential new opportunity for fraudulent attack.

b. Pressure to launch new services to gain competitive advantage often results in little attention to security or fraud initiatives.

c. This risk is compounded when these services are offered by new operators.

d. Key aspect of fraud management role is to be an integral part of the new product and service development process.

e. The Fraud Team needs to ensure they can determine the required points of control, measurement, and monitoring to ensure appropriate prevention initiatives are in place.

### 2. 7. 13 Evaluating New Products and Services: (elemen customer care, 2008)

a. To ensure maximum profitability of new products and services a risk evaluation is paramount as this enables both a revenue protection and fraud prevention strategy to be deployed across the various business segments.

b. This practice should be designed into the business processes so that the business can be proactive to fraud and revenue management issues rather than reactive.

c. The evaluation of new products, services and systems is a vital business process that should be undertaken prior to launch and continually assessed, it should never be viewed as a single activity.

d. The resulting losses from a product or service that has not been thought through properly and the potential fraud and security risks determined can result in large financial losses through process and procedure weaknesses, in addition, to losing customer confidence.

e. On some occasions, the need to get a new product or service to market will be greater than the requirement to build in fraud protection.

f. In these cases, a prior understanding of the functionality of the product will allow the fraud team to be proactive to instances of fraud.

### 2. 7. 14 Effective Measures – Detect and Protect: (Roberts, Dabija. 2009)

a. Operators need to implement a more Pro-active approach to fraud management.

b. Establish well documented, well communicated end to end processes across the product and service portfolio.

c. Develop effective monitoring tools and performance indicators - become proactive not reactive.

d. Perform timely reconciliation and provide management reporting capabilities.

e. Establish the root cause of the problems to ensure preventative measures can be implemented.

f. Enforce existing and introduce new policies and procedures.

g. Perform internal reviews of high risk activities as highlighted from the review and this training.

h. Identify measure, control and prevent to ultimately reduce exposure - risk management principles.

i. The need for greater internal communication within the business - cooperation - visibility - understanding.

j. Active participation by the Internal Audit, Ethics and Compliance functions regarding new products and services to ensure adequate levels of protection.

k. Adopt a multi disciplined approach - effective utilization of skill sets - subject matter experts (technical, IT Skills supporting the Fraud Team).

l. Define clear ownership and accountability for product and service integrity - the Risk Management function will never directly own a product or service!

### 2. 7. 15 Fraud Management Methodology in Developing Countries (Banjako, 2009):

#### *2. 7. 15. 1 Start up Operator:*

Startups tend to rely on high usage alerts based on call types, value, duration or even credit limits. This function often has close similarities to credit control and it is important to clearly define the role of the fraud team so that they can concentrate on managing fraud. There may be limited investigation depending upon the resources available to the operator. Investigations may be limited and focused on fact finding, resolving network issues, understanding customers and in some instances presenting cases for prosecution

In most cases the individuals with responsibility for fraud management in startup has an important role not only to lay the sound base for fraud management but also to define the next stages of fraud management as the company grows whilst protecting the company’s revenue with limited tools and resources.

### 2. 7. 15. 2 Established Operator:

An established operator will have defined the role of fraud management within the company and will be working to ensure that this is implemented in line with the changing business requirements and the fraud strategy. They would usually have a fraud management System or be in the process of selecting a system. The company will be experienced and perform a number of fraud management activities including using refined alert sets to reduce false positives, use previous fraud data to detect repeat fraudsters and be conversant with a variety of in house and external analysis tools. They would have built up relationship with external agencies and have a good understanding of the regulations that govern the operator. Investigations would be clearly defined and will often involve more than one person and include specialists areas such as network investigations, it security. Investigations may also be publicized within the company by highlighting key successes and cases prosecuted internally; their fraud management team will be experienced, have detailed procedures and be in contact with other departments and customers on a regular basis. There will be several key roles within the team to improve fraud detection and reporting capabilities. They would have a profiling database alerts and Fraud Intelligence.

established operator would usually have a fraud management system or be in process of selecting system, the company will be experienced and perform number of frau management activates, including using refined alert sets or reduce the false positives, but mainly they depend on high usage alerts, high usage cried alerts, investigation and fraud reporting.

### 2. 7. 15. 3 Best Practice:

Fraud Management methodologies have increased over the years. The methods and resources available to improve the management of fraud as listed in the diagram. It is important to understand that some best practice elements will not be practicable or even suitable for some operators depending on the environment and skill set available. Operators who undertake fraud management vary in what they do, some startups and established Telco's, enter into very advanced fraud management and use best practice that is drawn from experienced fraud and security professionals the stakes are high and every prompt is taken very seriously The fraud management cycle is one principle that has been used in the industry for some time (prevent-select-analysis-respond and measure) This are the key elements in successfully managing fraud. It is a continuous improvement cycle that integrates the varying methods and requires constant improvements/discussions, tolls, techniques, processes and people. No one method or tool will be wholly adequate. Only a fully integrated approach, combing a variety of approaches**.**

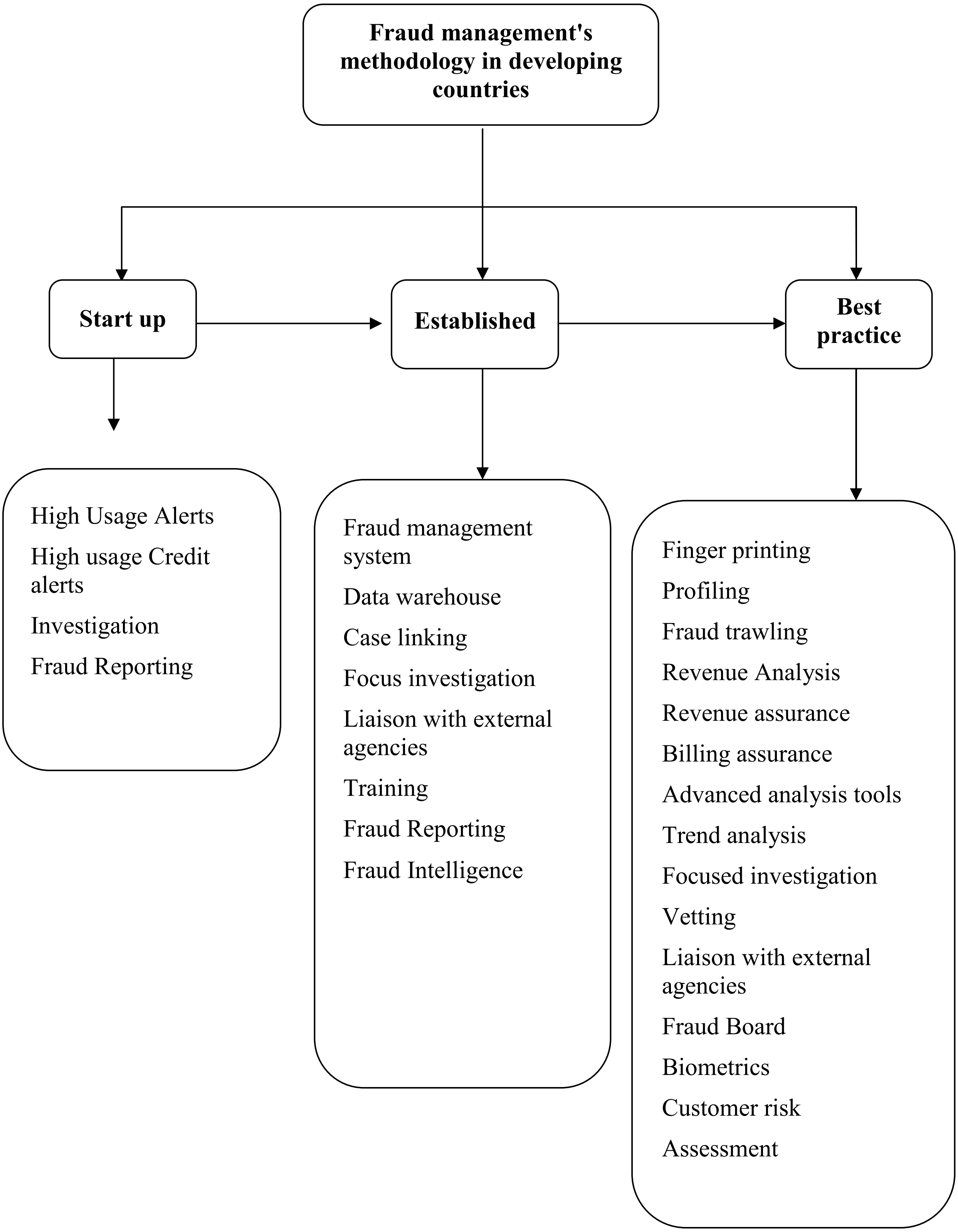

***Figure (2) Fraud management's methodology in developing countries***

# CHAPTER [3]

# RELATED WORK

A lot is written about how to detect fraud. However many authors, like Bologna and Lindquist (1995), state that prevention should take precedence over detection. The authors mean by fraud prevention creating a work environment that values honesty. This includes hiring honest people, paying them competitively, treating them fairly, and providing a safe and secure workplace.

In the Accountant '3 Guide to Fraud Detection and Control, Davia et al (2000) state that it is management's responsibility to allocate resources and emphasis to fraud-specific internal controls and to proactive fraud-specific examinations. These approaches are examples of prevention on one hand and detection on the other. The authors point out that it is a mistake to think in terms of one versus the other. Strong internal controls as fraud prevention are very important, but they are best reinforced by following fraud-specific examinations.

In the study conducted world wide by Price water house Cooper PwC ( PwC,2007) and study conducted in united state by ACFE(ACFE,2006), both speaks about detection. The studies investigate by means of surveys which are the most occurring means or methods that lead to fraud detection, or are believed to do so by the CFO's. The following are the findings of both studies.

About the way fraud is detected, both studies of PwC and the ACFE stress the importance of tips and chance. According to the ACFE report, an anonymous fraud hotline anticipates a lot of fraud damage. In the cases reviewed, organizations that had such hotlines, suffered a median loss of US$ 100. 000, whereas organizations without hot lines had a median loss of US$ 200. 000. At the PwC study, no less than 41 % of the fraud cases was detected by means of tip-offs or by accident. Internal audit and internal control systems can have a measurable impact on detecting fraud after chance related means. The more control measures a company puts in place, the more incidents of fraud will be uncovered.

Another recent study, performed by Ernst and Young, mentions preventing and detecting fraud. The global survey by Ernst and Young in 2006 revealed similar insights on fraud prevention factors. Respondents identify internal controls as the key factor to prevent and detect fraud. (Ernstand Young, 2006).

In anti fraud management survey conducted by BAKER TILLY (2008),The Majority of the companies (59%) of the represented by the survey perceive their greatest fraud threat to b from their own employees, the vast majority of the respondents (77%) stated that thy had participated in n investigation, indicting that companies are taking fraud seriously and investigated them. However ,only half of the respondents (51%) stated that they have an incident response plane in place, about the company's exposure to fraud ,respondents preserved that their companies are most susceptible to internal or employee fraud, and nearly half of the respondents were unable to quantify the impact of fraud in their company, and bout fraud risk management and assessment, less half of the respondents reported having completed some sort of formalized fraud risk assessment .An over helming percentage of respondents feel like they could be doing more regards to fraud risk management.

In the global fraud report economist intelligence unit survey results(2010) , the middle east overview of fraud , at first glance the global fraud survey figures for the middle suggest that the region is not doing badly compared to other parts of the world. The over all incidence is the same as the global average. Although companies in the region face significant problem with information theft and physical theft, so doe every one else and the Middle East figures only slightly above normal.

The region incidence of seven of eleven frauds covered in the survey are below average, and for three –management conflict of interest (12%), vender fraud (9%), and IP theft 2% , the middle east has the lowest rate of any region.

Other data points in the opposite direction: 45% of all companies had an employee commit fraud writhen the last year, meaning that employees mad up 61% of known perpetrators, in both cases the highest figures for any region. The Middle East also had the second highest figure after Africa. - For companies suffering at least some financial loss (70%).

Despite apparently having performed relatively well compared to the rest of the world, survey respondent in the Middle East understand that theirs region where fraud risk are higher than normal and it is necessary to protect companies accordingly. Forty present of the Middle East respondents said that the fraud had grown worse at there companies than the past year.

Beware that all above mentioned suggestions concerning detection and prevention of fraud, concern fraud detection/prevention and further, are the results of non-academicals research. In the next section. an overview of the academic literature concerning fraud detection and prevention is given.

To gain a clear view of the current situation of research table 1 is created by Mieke.jans, Nadine.Lybaret and Koen.Vanhoof (2009) , This will provide us with some insights of the implicitly followed methodology in current literature. The table provides us with the author(s) in alphabetical order, the application domain, whether it concerns internal or external fraud, whether the objective is fraud detection or prevention, and which technique is used. The researcher expects most articles to deal with fraud detection rather than prevention and fraud management. . .

Concerning the techniques used, an intensively explored method is neural networks. The studies of Davey et al. (1996) and Hilas and Mastorocostas (2008) (telecommunications fraud), Dorronsoro et al. (1997) (credit card fraud), and Fanning and Cogger (1998), Green and Choi (1997) and Kirkos et a1. (2007) (financial statement fraud) all use neural network technology for detecting fraud in different contexts. Lin et al. (2003) apply a fuzzy neural net, also in the domain of fraudulent financial reporting. Both Brause et al. (1999) and Estevez et al. (2006) use a combination of neural nets and rules. The latter use fuzzy rules, where the former use traditional association rules. Also He et a1. (1997) apply neural networks: a multi –layer perception network in the supervised component of their study and Kohonen's self –organization maps for the unsupervised parts. Like He et al. (1997) apply in their unsupervised parts, Brockett et al. (1998) apply Kohnen's self organizing feature maps(a form of neural network technology) to uncover phony claims in the domain of automobile insurance. This is also what Zaslavsky and Stizhk (2006) suggest later, in 2006, in methodological paper to detect credit card fraud. Quah and sriganesh (2008) follow this suggestion in an empirical paper on understanding spending patterns to decipher potential fraud cases. A Bayesian learning neural network is implemented for credit card fraud detection by Maes et al. (2002) (aside to an artificial neural network), for uncollectible telecommunications accounts (which is not always fraud) by Ezawa and Norton (1996), for financial statement fraud by Kirkos et a1. (2007) and for automobile insurance fraud detection by Viaene et al. (2005) and Viaene et al (2002).

In a related field of Viaene et al. (2005) 's automobile insurance fraud, Bermudez et l. (2007) use an asymmetric or skewed logit link to fit a fraud database from the Spanish insurance market. Afterwards they develop Bayesian analysis of this model. In related field Major and Riedinger (2002) presented a tool for the detection of medical insurance fraud. They proposed a hybrid knowledge/statistical-based system, where expert knowledge is integrated with statistical power. Another example of combining different techniques can be found in Fawcett and Provost (1997). A series of data mining techniques for the purpose of detecting cellular clone fraud is hereby used. Specifically, a rule-learning program to uncover indicators of fraudulent behavior from a large database of customer transactions is implemented. From the generated fraud rules, a selection has been made to apply in the form of monitors. This set of monitors profiles legitimate customer behavior and indicate anomalies. The outputs of the monitors, together with labels on an account's previous daily behavior, are used as training data for a simple Linear Threshold Unit (LTU). The LTU learns to combine evidence to generate high-confidence alarms. The method described above is an example of a supervised hybrid as supervised learning techniques are combined to improve results. In another work of Fawcett and Provost (1999), Activity Monitoring is introduced as a separate problem class within data mining with a unique framework. Fawcett and Provost (1999) demonstrate how to use this framework among other things for cellular phone fraud detection.

Another framework presented, for the detection of healthcare fraud, is a process-mining framework by Yang and Hwang (2006). The framework is based on the concept of clinical pathways where structure patterns are discovered and further analyzed.

The fuzzy expert systems are also experienced with in a couple of studies. So there are Derring and Ostaszewski (1995), Deshmukh and Talluru (1998), Pathak et al. (2003), and Sanchez et al (2008). The latter extract a set of fuzzy association rules from a data set containing genuine and fraudulent credit card transactions. These rules are compared with the criteria which risk analyst apply in there fraud analysis process. The research is therefore difficult to categorize as "detection" "prevention" or both. The researcher adopted the authors' own statement of contribution in both fraud detection and fraud prevention. Derrig and Ostazewaski (1995) use fuzzy clustering and therefore apply a data mining technique performing a descriptive task, where the other techniques (but Sanchez et al. (2008) perform a predictive task.

Stolfo et al. (2000) delivered some interesting work on intrusion detection. They provided a framework, MADAM ID, for Mining Audit Data for Automated Models for Intrusion Detection. However intrusion detection is associated with fraud detection, this is a research area on its own and the researcher does not extend his scope to this field. Next to MADAM ID, Stolfo et a1. (2000) discuss the results of the JAM project. JAM stands for Java Agents for Meta-Learning. JAM provides an integrated meta-learning system for fraud detection that combines the collective knowledge acquired by individual 1ocal agents. In this particular case, individual knowledge of banks concerning credit card fraud is combined. Also Phu et al(2004) apply a meta –learning approach, in order to detect fraud and not only intrusion. The authors bas their concept on the science fiction novel Minority Report and compare with the base classifiers with the novel's "precogs". The used classifiers are the naive Bayesian algorithem, C4. 5 and back propagation natural networks. Results from publicly available automobile insurance fraud detection data set demonstrate that the stacking-bagging performs better in term of performance as well as in term of cost saving.

Cahill et al. (2000) design a. fraud signature, based on data of fraudulent calls, to detect telecommunications fraud. For scoring a call for fraud its probability under the account signature is compared to its probability under a fraud signature. The fraud signature is updated sequentially, enabling event-driven fraud detection.

Rule-learning and decision tree analysis is also applied by different researchers, e. g. Kirkos et al. (2007), Fan (2004), Viaene et al. (2002), Bonchi et al. (1999) and Rosset et al. (1999). Viaene et al. (2002) actually apply different techniques in their work, from logistic regression, k-nearest neighbor, decision trees and Bayesian neural network to support vector machine, naive Bayes and tree-augmented naive Bayes. Also in Viaene et al. (2007), logistic regression is applied.

Link ana1ysis comprehends a different approach. It relates known fraudsters to other individuals, using record linkage and social network methods (Wasserman and Faust, 1998). Cortes et al. (2002) find the solution to fraud detection in this field. The transactional data in the area of telecommunications fraud is represented by a graph where the nodes represent the transactors and the edges represent the interactions between pairs of transactors. Since nodes and edges appear and disappear from the graph through time, the considered graph is dynamic. Cortes et al. (2002) consider the subgraphs centered on all nodes to define communities of interest (COI). This method is inspired by the fact that fraudsters seldom work in isolation from each other.

To continue with link analysis, Kim and Kwon (2006) report on the Korean Insurance Fraud Recognition System that employs an unsupervised three stage statistical and link analysis to identify presumably fraudulent claims. The government draws on this system to make decisions. The authors evaluate the system and offer recommendations for improvement.

Bolton and Hand (2001) are monitoring behavior over time by means of Peer Group Analysis. Peer Group Analysis detects individual objects that begin to behave in a way different from objects to which they had previously been similar. Another tool Bolton and Hand (2001) develop for behavioral fraud detection is Break Point Analysis. Unlike Peer Group Analysis, Break Point Analysis operates on the account level. A break point is an observation where anomalous behavior for a particular account is detected. Both the tools are applied on spending behavior in credit card accounts.

Also Murad and Pinkas (1999) focus on behavioral changes for the purpose of fraud detection and present three-level-profiling. As the Break Point Analysis from Bolton and Hand (2001), the three-level-profiling method operates at the account level and it points any significant deviation from an account's normal behavior as a potential fraud. In order to do this, 'normal' profiles are created (on three levels), based on data without fraudulent records. To test the method, the three-level-profiling is applied in the area of telecommunication fraud. In the same field, also Burge and Shawe- Taylor (2001) use behavior profiling for the purpose of fraud detection by using a recurrent neural network for prototyping calling behavior. Two time spans are considered at constructing the profiles, leading to a current behavior profile (CBP) and a behavior profile history (BPH) of each account. In a next step the Hellinger distance is used to compare the two probability distributions and to give a suspicion score on the calls.

A brief paper of Cox et al. (1997) combines human pattern recognition skills with automated data algorithms. In their work, information is presented visually by domain-specific interfaces. The idea is that the human visual system is dynamic and can easily adapt to ever-changing techniques used by fraudsters. On the other hand have machines the advantage of far greater computational capacity, suited for routine repetitive tasks.

Four last studies i would like to mention are those of Tsung et al. (2007) and Brockett et al. (2002). Hooges et al. (2007) and Jaszczak et al. (2008). Tsung et al. (2007) apply manufacturing batch techniques to the field of fraud detection. They use the batch library method. Brockett et al. (2002) use a principal component analysis of RIDIT scores to classify claims for automobile bodily injury. Hooges et al. (2007) presents a genetic algorithm approach to detect financial statement fraud. They find that exceptional anomaly scores are valuable metrics for characterizing corporate financial behavior and that analyzing thee scores over tome represents and effective way of detecting potentially fraudulent behavior. Juszczak et el. (2008) at last apply many different classification techniques in supervised two-class setting asemi-supervised one-class setting in order to compare performance of thee techniques and setting.

***Table (1): Fraud detection/prevention literature overview***

| Author | Application Domain | Internal/ External | Detection/ Prevention | Technique | Task |
|---|---|---|---|---|---|
| Bermudez et al (2007) | Automobile insurance fraud | external | Detection | Skewed Logit Link and Bayesian | predictive |
| Bolton and Hand (2001) | Credit Card Fraud | External | Detection | Peer Group Analysis and Break Point | Predictive |
| Bonchi et al. (1999) | Fiscal Fraud | External | Detection | Decision Tree | Predictive |
| Brause et al. (1999) | Credit Card Fraud | External | Detection | Rules and Neural Network | Predictive |
| Brockett et al. (1998) | Automobile Insurance Fraud | External | Detection | Kohonen's Self-Organizing Map | Predictive |
| Brockett et al. (2002) | Automobile Insurance Fraud | External | Detection | Principal Component Analysis | Predictive |
| Burge and Shawe- Taylor (2001) | Telecommunication Fraud | External | Detection | Unsupervised Neural Network | Predictive |
| Cahill et al (2002) | Telecommunications Fraud | External | Detection | Profiling by means of signatures | Predictive |
| Cortes et al. (2002) | Telecommunications Fraud | External | Detection | Dynamic Graphs | Predictive |
| Cox et al. (1997) | Telecommunications Fraud | External | Detection | Visual Data Mining | Descriptive |

| Author | Application Domain | Internal/ External | Detection/ Prevention | Technique | Task |
|---|---|---|---|---|---|
| **Continue…** | | | | | |
| Davey et al. (1996) | Telecommunications Fraud | External | Detection | Neural Network | Predictive |
| Derrig and Ostaszewski (1995) | Automobile Insurance Fraud | External | Detection | Fuzzy Set Theory | Descriptive |
| Deshmukh and Talluru (1998) | Financial Statement Fraud | Internal | Detection | Rule-based Fuzzy Reasoning System | Predictive |
| Dorronsoro et al. (1997) | Credit Card Fraud | External | Detection | Neural Network | Predictive |
| Estevez et al. (2006) | Telecommunications Fraud | External | Detection | Fuzzy Rules and Neural Network | Predictive |
| Ezawa and Norton (1996) | Uncollectible Telecommunications Accounts | External | Detection | Bayesian Neural Network | Predictive |
| Fan (2004) | Credit Card Fraud | External | Detection | Decision Tree | Predictive |
| Fanning and Cogger (1998) | Financial Statement Fraud | Internal | Detection | Neural Network | Predictive |
| Fawcett and Provost (1997) | Telecommunications Fraud | External | Detection | Rules, Monitors and Linear Threshold Unit | Predictive |
| Fawcett and Provost (1999) | Telecommunications Fraud | External | Detection | Activity Monitoring | Predictive |
| Green and Choi (1997) | Financial Statement | Internal | Detection | Neural Networks | Predictive |
| He et al. (1997) | Health Care Insurance Fraud | External | Detection | Neural Networks | Predictive |
| He et al. (1997) | Health Care Insurance Fraud | External | Detection | Kohonen's Self-Organizing Map | Descriptive |

| Author | Application Domain | Internal/ External | Detection/ Prevention | Technique | Task |
|---|---|---|---|---|---|
| **Continue…** | | | | | |
| Hilas and Mastorocostas (2008) | Telecommunication fraud | External | Detection | Neural Network and clustering | predictive |
| Hoogs et al (2007) | Financial Statement Fraud | Internal | Detection | A Genetic Algorithm Approach | predictive |
| Juszczak et al (2008) | Credit card fraud | External | Detection | Many different classification techniques | predictive |
| Kim and Kwon (2006) | Insurance Fraud | External | Detection | Insurance Fraud Recognition System (Korea) | Predictive |
| Kirkos et al. (2007) | Financial Statement Fraud | Internal | Detection | Decision Tree, Neural Network and Bayesian Belief Network | Predictive |
| Lin et al. (2003) | Financial Statement Fraud | Internal | Detection | Fuzzy Neural Network | Predictive |
| Maes et al. (2002) | Credit Card Fraud | External | Detection | Neural Network and Bayesian Belief Network | Predictive |
| Major and Riedinger (2002) | Health Care Insurance Fraud | External | Detection | Electronic Fraud Detection (EFD) | Predictive |
| Murad and Pinkas (1999) | Telecommunications Fraud | External | Detection | Three Level Profiling | Predictive |
| Pathak et al. (2003) | Insurance Fraud | External | Detection | Fuzzy logic based expert system | Predictive |
| Phua et al(2004) | Automobile insurance fraud | External | Detection | Meta-classifiers | predictive |
| Sriganesh (2008) | Credit card fraud | External | Detection | Self organizing maps | descriptive |
| Rosset et al. (1999) | Telecommunications Fraud | External | Detection | Rules | Predictive |
| Sanchez et al. (2008) | Credit card fraud | External | Detection and prevention | Fuzzy rules | descriptive |

| Author | Application Domain | Internal/ External | Detection/ Prevention | Technique | Task |
|---|---|---|---|---|---|
| **Continue…** | | | | | |
| Stolfo et al. (2000) | Credit Card Fraud and Intrusion | External | Detection | Meta-classifiers | Predictive |
| Tsung et al. (2007) | Telecommunications Fraud | External | Detection | Batch Library Method | Predictive |
| Viaene et al. (2005) | Automobile Insurance Fraud | External | Detection | Bayesian Neural Network | Predictive |
| Viaene et al. (2002) | Automobile Insurance Fraud | External | Detection | Logistic Regression, k-Nearest Neighbor, Decision Tree, Bayesian Neural Network, SVM, Naïve Bayes, and tree-augmented Naïve Bayes | Predictive |
| Viaene et al. (2007) | Automobile Insurance Fraud | External | Detection | Logistic Regression | Predictive |
| Yang and Hwang (2006) | Health Care Insurance Fraud | External | Detection | Frequent Pattern Mining | Predictive |

Source: (International journal of digital accounting research)

If we summarize existing academic research by looking at Table 1, we arrive at the conclusion that merely all research is conducted in the field of external fraud. Concerning internal fraud, there is a gap in the academic literature. Only six articles on internal fraud were found and they address only one kind of internal fraud: statement fraud. It is confirmed by Table 1. All research aims at providing a detection tool, only two articles incorporate the importance of prevention. As a last observation, one notices that all articles found apply data mining techniques. And about the studies of PwC and ACFE, assets misappropriation which is a form of transactional fraud is the most prevalent kind of internal fraud . this is remarkable divergence of non-academic research where the internal control was pointed as an effective tool after chance related means (PwC2007).

# CHAPTER [4]

# JAWWAL PROFILE

**4. 1 Development Timeline of Jawwal**

**4. 2 Jawwal Subscribers and Market Penetration Rate**

**4. 3 Postpaid and Prepaid Subscribers**

**4. 4 Jawwal Revenues**

**4. 5 Jawwal Anti Fraud Section Operations**

**4. 6 Jawwal Bad Debit**

Jawwal the mobile arm of Paltel, received its territorial license concession in 1996, and launched its services in 1999. Jawwal was founded as a joint venture between Paltel (65%), and the Palestinian Investment Fund received 35% of the shares. Later, in 2003 the PIF sold its portion to Paltel for USD 43 millions. Since its' launch Jawwal has been faced with fierce competition from the Israeli operators, and has had no choice but to employ every possible means at hand to enhance its competition stand following its rollout, it continues to develop its network and services to satisfy the customers' needs, Jawwal coverage 97% from the Palestinian territories (Rabayah, Awad and Kareem, 2008). .

## 4. 1 Development timeline of Jawwal: (Rabayah, Awad and Kareem, 2008)

a. Jawwal contracted Ericson in its first roll out phase of the GSM network for USD 40 million, a deal which was signed in 1999. Jawwal also contracted Alcatel to supply the switching equipment. The first phase had a capacity of about 120,000 subscribers.

b. In May 2001 a further USD12 million contract was signed with Ericson to double network capacity to 220,000 and install GPRS-enabled equipment. Palcel contracted Alcatel once more in December 2004 to replace part of its GSM network infrastructure in Gaza with GPRS-enabled equipment for an undisclosed 'multi-million dollar' sum.

c. Commercial GPRS services were launched shortly afterwards, initially to post-paid users only. The rollout of new lines then came to an abrupt halt due to Israeli customs blocking the delivery of equipment necessary to expand its network. As a result Palcel stopped selling new lines in the fourth quarter of 2005.

d. The imports were eventually received in December that year, 18 months late, leading Palcel to significantly up its CAPEX for 2006 to 1OD46 million (USD64.5 million), from JOD 16. 5 million a year earlier, and announce a USD23 million deal with Ericson to commence the third stage of its network expansion, under which it increased capacity to 1. 5 million users and provided an upgrade to EDGE technology.

e. At the end of December 2006 Jawwal's network consisted of around 373 base stations providing coverage of 98% of Palestinian Territories.

f. Intense competition with the Israeli providers has prompted Pakel to slash its call costs and ramp up services. It offers a portfolio of wireless services via GSM, GPRS and EDGE, and has roaming agreements with 239 operators in 112 countries.

g. It has launched numerous promotions offering discounted calls, including a 33% reduction to users calling numbers on Israeli networks in the first quarter of 2006, and exploits its status as a subsidiary of Paltel to offer the cheapest rates for calling Palestine fixed lines.

h. In 2006 Jawwal launched several new services including MMS, voice mail, an up-to-the minute news service (Emailak) for post-paid subscribers, billing via e-mail, group calls and other voice call services, in addition to banking services and bill paying options through the internet and via A TMs.

i. During 2007 the cellco says it continued to provide cutting-edge telecoms, IT services, data communications and other value added services including the planned deployment of '3G' technologies to meet customer needs in all Palestinian areas. In this respect, Jawwal says it will deploy 3G technology whenever it obtains the necessary frequencies.

j. In 2007 Jawwal signed roaming contracts with Cellcom to provide roaming services in Palestinian areas that are currently not covered by its network, namely in the city of Jerusalem and areas within the Green Line and to circumvent the Israeli obstacles that prevent Jawwal from expanding its services within these areas. The agreement adds to a much earlier contract signed with Partner in 2000.

k. In 2008 Jawwal and Paltel’s infrastructure suffered severe damage caused by the continuous Israeli shelling on Gaza Strip which resulted in an interruption of some Paltel and Jawwal’s services. The interruption was a direct result of the continuous shelling on Jabalia’s exchange which destroyed Jawwal’s mobile towers.

l. In 2008 Jawwal Company announced launching its Military Plan, a special package with its new features provided for the Palestinian Security men to honor them in the Palestinian Independence Day, also has launched Fleet management service in cooperation with Hulul and Wasel companies. This ideal technology will help the companies and institutions to monitor and mange their fleet of vehicles more efficiently using the Global Positioning System in addition to the fleet management system. Jawwal activated the international roaming service for all to providing direct calls with the Israeli operator "Mirs", where now all Jawwal's subscribers are able to make and receive calls with. For any one who is interested in this service should dial 057 before any number

m. In 2009, Jawwal started implementing its plans concerning its network expansion, in order to support the series of offers and campaigns which will be offered to more than one million and a half subscribers. This step came after the delivery of technical equipments which will enable the network expansion to handle the growth in its subscribers' base, in November 19 2009 Mr. Sabih Masri, Chairman of the Board of Paltel announced the termination of the Paltel-Zain share swap agreement, and that is due to the lapse of the period granted within the terms of the agreement signed between Paltel and Zain. The time period allocated passed without fulfilling all the necessary requirements and procedures to conclude the deal(Jawwal websit)

n. During 2010 Jawwal has started implementing phase 10 of its plan for updating its network, which will support the quality of services provided for more than 2,000,000 customers, after signing a more than $15 million contact with Ericson company. This comes after 10 years of successes to more evolve and improve Palestinian usage of IT.(Jawwal website)

o. In October 2010 Jawwal has launched "Roaming on Airplanes" service for postpaid subscribers, one of many special services they offer for subscribers, This service has been launched with cooperation with "On Air", one of the largest on airplanes services providers which specializes in providing Internet (GPRS), making and receiving calls and SMS services on airplanes on more than 4000 KM height of ground, by preparing 40 airplanes flying over 200 countries with special equipments; This service is now available on many airplanes of Saudi, Jordan, Oman, Qatar, Libyan, Kuwaiti national airlines in addition to British and Portugal airlines and Asia Air.(Jawwal websit)

## 4. 2 Jawwal subscribers and market penetration rate:

According to Arab advisor group strategic research (Arab advisor group, 2010), the Palestine's cellular penetration reached an estimated 62% by end of first quarter, 2010 with the market adding 402, 000 new lines. Paltel's cellular subsidiary, Jawwal, added 287, 610 lines in H1 2010 to reach a total of around 2. 07 million lines and a market share of 82%. While Palestine's new entrant, Wataniya Mobile, reported serving 243, 000 lines by H1 2010 since it first launched its services, in November 2009.

Palestine's total estimated cellular market penetration rate soared to 62% by end of June 2010. In 2009, the Arab Advisors Group estimated that the total cellular additions were 587, 000 with a record growth of 38. 2%. During the first quarter of 2010, the Arab advisors Group estimates that Jawwal, Wataniya Mobile and the four Israeli operators have added 402, 000 cellular subscribers during 2010's first half to exceed the 2. 5 million mark by end of June 2010. Table (2) shows more details.

***Table (2): Palestine cellular subscribers (2007-H12010)***

| | **2008** | **2009** | **H1 2010** |
|---|---|---|---|
| total cellular subscribers (2007-H12010) | 1, 537 | 2, 124 | 2, 526 |
| Added subscribers | 210 | 587 | 402 |
| Growth % | 15. 80% | 38. 20% | 18. 90% |
| cellular market penetration | 40% | 53% | 62% |

Source: (Arab advisor group, 2010)

The two Palestinian operators registered solid growth during 2010's first half. Jawwal started the year with 1.784 million subscribers and added 287, 610 subscribers to reach a total of 2.07 million by end of June 2010. Wataniya Mobile reported reaching a subscriber base of 243,000 lines by end of June 2010 since its commercial launch in November 10, 2009. This translates into an estimated market share of 9. 6% by end of H1 2010. Israeli operators' market share dropped to an estimated 8.4% by end of June 2010. Table (3) shows more details.

***Table (3): Jawwal and Wataniya market shares***

| | **2008** | **2009** | **2010** |
|---|---|---|---|
| Jawwal lines | 1, 314. 41 | 1, 783. 94 | 2, 071. 55 |
| Added lines | | 469. 535 | 287. 61 |
| Growth% | | 35. 70% | 16. 10% |
| Market share% | 85. 50% | 84% | 82% |
| Wataniya lines | | 111 | 243 |
| Added lines | | | 132 |
| Growth% | | | 118. 90% |
| Market share% | | 5. 20% | 9. 60% |
| Israeli Operators lines | 222. 59% | 229. 059 | 211. 7307 |
| Added lines | | 6. 465 | -17. 328 |
| Growth% | | 2. 90% | -7. 60% |
| Market share% | 14. 50% | 10. 80% | 8. 40% |

Source: (Arab advisor group, 2010)

## 4. 3 Postpaid and prepaid subscribers:

Both, Jawwal’s prepaid and postpaid lines grew, at different rates. While prepaid lines grew by 15. 4% during H1 2010, postpaid lines grew by 22. 4%. Prepaid additions constituted 86% of the total additions during H1 2010 compared to 98. 1% during 2009. Jawwal added 247, 480 prepaid lines during H1 2010, compared to 40, 130 postpaid lines during the same period. Jawwal’s prepaid lines constituted 89. 4% of the total subscribers’ base by end of June 2010. Table (4) shows more details

***Table (4) Jawwal's lines breakdown (2007-H12010)***

| | **2008** | **2009** | **H1 2010** |
|---|---|---|---|
| Jawwal lines | 1, 314. 41 | 1, 783. 94 | 2, 071. 55 |
| Added lines | 292. 925 | 469. 535 | 287. 61 |
| Growth % | 28. 70% | 35. 70% | 16. 10% |
| Prepaid lines | 1, 144. 26 | 1, 604. 96 | 1852. 437 |
| Added lines | 254. 256 | 460. 694 | 274. 48 |
| Growth % | 28. 60% | 40. 30% | 15. 40% |
| % Of total lines | 87. 10% | 90% | 89. 40% |
| %Of total additions | 86. 80% | 98. 10% | 86% |
| Postpaid lines | 170. 143 | 178. 984 | 219. 114 |
| Added lines | 38. 669 | 8. 841 | 40. 13 |
| Growth % | 29. 40% | 5. 20% | 22. 40% |
| % Of total lines | 12. 90% | 10% | 10. 60% |
| %Of total additions | 13. 20% | 1. 90% | 14% |

Source: (Arab advisor group, 2010)

## 4. 4 Jawwal revenues:

Jawwal generated JD 120. 611 million (US$ 169. 875 million) in revenues during H1 2010, a growth rate of 12% over H1 2009's figure. Monthly cellular ARPU during H1 2010 reached US$ 14. 5 down from US$ 17. 14 in H1 2009. The Arab Advisors Group believes that the drop in ARPU resulted from Wataniya Mobile launching its services and commencing intense local competition in Palestine's cellular market among Palestinian operators. Table (5) shows more details

***Table (5): Jawwal revenues (2007-H12010)***

| | **2008** | **2009** | **H1 2009** | **H1 2010** |
|---|---|---|---|---|
| Jawwal lines | 1, 314. 41 | 1, 783. 94 | 1, 589, 390 | 2, 071. 55 |
| Jawwal revenues (us$) | 282, 779 | 327, 754 | 151, 663 | 169, 875 |
| Growth | - | 15. 90% | - | 12% |
| Jawwal ARPU(US$) | 19, 97 | 17, 41 | 17. 14 | 14. 51 |
| Growth in ARPU (us$) | 11% | -13% | - | -15. 40% |

Source: (Arab advisor group, 2010)

## 4. 5 Jawwal anti fraud section operations:

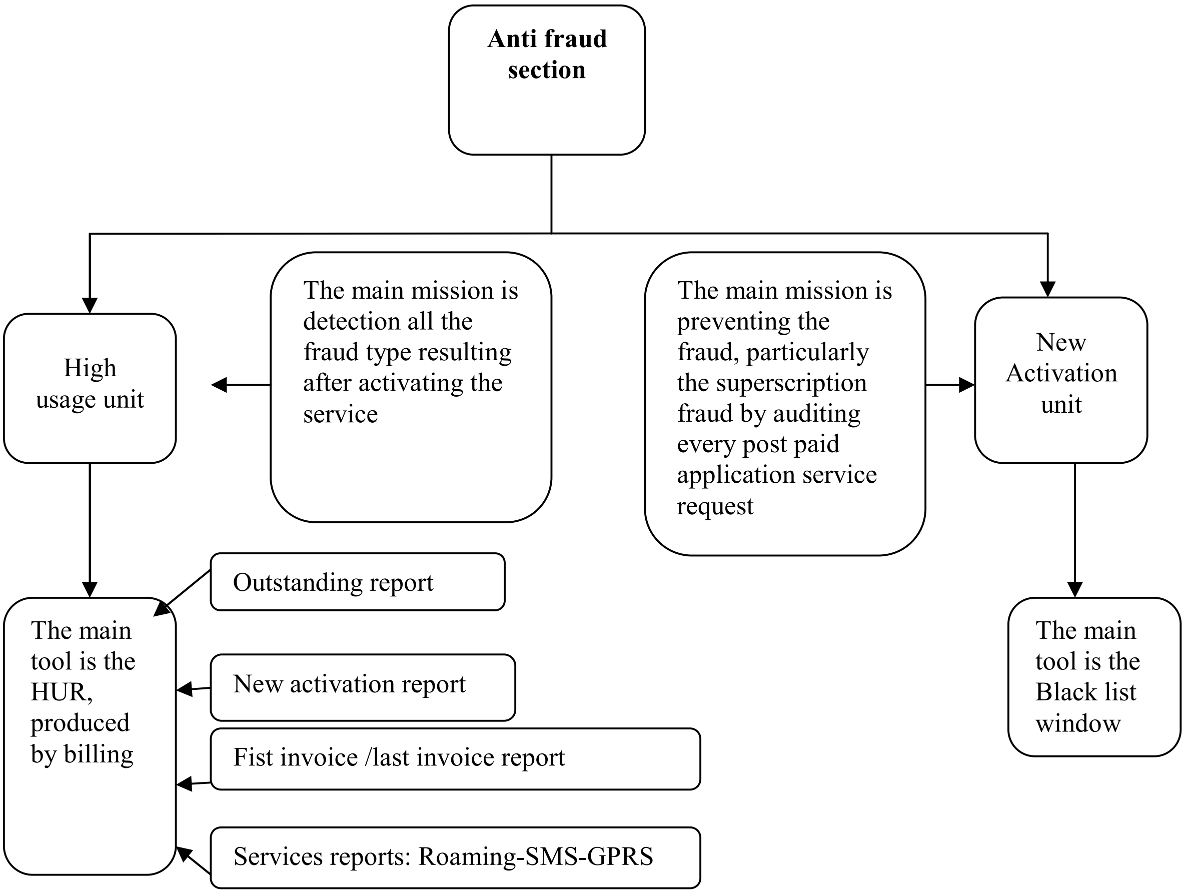
Anti fraud section
High usage unit
The main mission is detection all the fraud type resulting after activating the service
The main mission is preventing the fraud, particularly the superscription fraud by auditing every post paid application service request
New Activation unit
Outstanding report
The main tool is the HUR, produced by billing
New activation report
Fist invoice /last invoice report
Services reports: Roaming-SMS-GPRS
The main tool is the Black list window

*Figure (3): Jawwal anti fraud section operations*

Jawwal fraud prevention and detection targeted the postpaid service, since the prepaid services fraud attack are not critical at Jawwal operator

preventing the fraud particularly the new subscriptions fraud by auditing the new service requests on the black list program, then reviewing the validation of the subscription form documents wither it is for the individual subscription or corporate subscription limits the problem of this type of fraud, which was the main fraud type before five years

Detecting the fraud by using the different types of the HUR, still lack the efficiency, since the theses reports treated manually in addition to some mistakes like not accurate amounts, and the posting delaying of the CDRs, may be fond, this is will affect the process of discovering the whole HU, and fraudulent cases.

## 4. 6 Jawwal bad debit:

The table below clarifying the amount of Jawwal bad debit up to December 2008:

***Table (6): JAWWAL bad debit up to December 2008***

| Year | Bad debit up to 31/7/2007 | Collection ratio 2008 | Bad debit up o 31/7/2008 | Net bade up to 31/12/2008 | Expected collection ration |
|---|---|---|---|---|---|
| 2000 | 14373801 | 5% | 13682434 | 13641004 | 1% |
| 2001 | 3, 249, 110 | 3% | 3151918 | 3142034 | 1% |
| 2002 | 4693367 | 4% | 4484053 | 449765 | 1% |
| 2003 | 1045048 | 8% | 966315 | 948472 | 2% |
| 2004 | 1286143 | 18% | 1070274 | 986480 | 5% |
| 2005 | 4648933 | 18% | 3857622 | 3590635 | 8% |
| 2006 | 27190051 | 64% | 10273623 | 9134707 | 10% |
| 2007 | 34721049 | 52% | 18068974 | 16713558 | 15% |
| 2008 | | | 20676742 | 18425263 | 19% |

Source: (Jawwal internal report)

As we stated before, Bad debt has a direct cost to the company, and the levels vary from Operator to Operator- good levels are <1% averaging 1-3% from revenue, Jawwal company is reluctant to express it is latest amount of bad debit, but the numbers above clarify that there is amounts of fraud losses are hidden in it, since Jawwal dos not distinguish between the bad debits losses and fraud losses, but as the collection ratio of the bad debit form year 2000-2005. Vary from 1%-8%, this indicate that there are uncollectable amount, and from the researcher point view classified as fraud losses, the large bad debit numbers approves Jawwal need for more efficient collection credit plans, and anti fraud tools.

# CHAPTER [5]

# METHODOLOGY

**5 . 1 Research methodologies**

**5 . 2 Questionnaire content**

**5 . 3 Content Validity of the Questionnaire**

**5 . 4 Statistical Validity of the Questionnaire**

This chapter describes the methodology that was used in this research. The adopted methodology to accomplish this study uses the following techniques: the information about data collection methodology, research population, questionnaire design, statistical data analysis, content validity and pilot study.

## 5 . 1 Research methodologies:

### Data Collection Methodology:

In order to collect the needed data for this research, we use the secondary resources in collecting data such as books, journals, statistics and web pages, in addition to preliminary resources that not available in secondary resources through distribute questionnaires on study population in order to get their opinions about fraud detection at Jawwal company. Research methodology depends on the analysis of data on the use of descriptive analysis, which depends on the poll and use the main program (SPSS).

### Population and sample size:

The population includes Jawwal employees from West bank and Gaza strip, the number of the employees is around 850 according to Jawwal internal report. The population of the targeted department is 418 employee, we select random sample with size (200) employees and (200) questionnaires were distributed via emails to the research population and (170) questionnaires are received, and the following table illustrated the properties of the samples:

***Table (7): Properties of the samples***

| Department/section | Original number | Number of respondents | Ratio of respondents |
|---|---|---|---|
| Sales | 271 | 96 | 35% |
| Due collection | 13 | 5 | 38% |
| Anti fraud | 11 | 9 | 81% |
| Risk operation | 47 | 17 | 36% |
| Complaints | 25 | 9 | 36% |
| Dealers | 41 | 34 | 82% |
| **Total** | **418** | **170** | |

## - Primary information:

## 1- Department/section:

***Table (8): Department/section***

| | Frequency | Valid Percent |
|---|---|---|
| Sales | 96 | 56. 5 |
| Due collection | 5 | 2. 9 |
| Anti fraud | 9 | 5. 3 |
| Risk operation | 17 | 10. 0 |
| Complaints | 9 | 5. 3 |
| Dealers | 34 | 20. 0 |
| **Total** | 170 | 100. 0 |

The results shows that 56% from the respondents from sales departments and if we add the 20% from dealers department which they are also considered part from the sales department we will get total of 76% of the respondents form the sales operation. This strengthens the fact that Jawwal main interest is still the sales operation, and the sales is the biggest department

a. According to internal static's Jawwal employees is about 850 employees, sales employee is around 315

b. The anti fraud, complaints, and the risk operation are sections under customer care umbrella, the total percent of the answers around 20%. This indicates that the sales in the bottom line, meanwhile customer care department come o the second or the third step according to the numbers of employees.

c. The results in the table agreed with the fiber optic association, (FOA, 2010) which said that seventeen percent of the industry's employees are in sales and related occupations, these workers, such as sales representatives and retail salespersons, are responsible for selling telecommunications and related services to businesses and residential customers

## 2- Experience:

***Table (9): Experience of the respondents***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Less than year | 14 | 8. 2 |
| 1-3 years | 35 | 20. 6 |
| 3-5 years | 47 | 27. 6 |
| More than 5 years | 74 | 43. 5 |
| **Total** | 170 | 100. 0 |

43% from the respondents were employees spent more than 5 year at Jawwal, this refers to fact that when Jawwal lunched its service at 1999, it is recruited large number of employees, they are considered now professional experts, and this is to share the opinion with the Robb Mattison (Mattison, 2009 p 22), he said "in general, people involved in revenue assurance have been working from three to ten years, meaning that the majority of revenue assurance professionals are in mid-20s mid 30s age group".

## 3- Qualifications:

***Table (10): Qualifications of respondents***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| **Diploma** | 11 | 6. 5 |
| **Bachelor's degree** | 148 | 87. 1 |
| **Post graduate studies** | 11 | 6. 5 |
| **Total** | 170 | 100. 0 |

Regarding the academic qualifications, 44% are holding bachelors' degree, graduating from commerce faculty in general, another information's should be mentioned, is the new trend toward the post graduate studies within the employees, that results in harmonize with Robb Mattison, GRAPA, revenue assurance (Mattison, 2009 P-22), he said the educational background of most revenue assurance professionals is higher than that of most "typical" employees. The vast majority of revenue assurance practitioners have a four-year college degree and almost half of them also have advanced degree.

## 4- Age Group:

*Table (11): Age Group of the respondents*

| | Frequency | Valid Percent |
|---|---|---|
| **20-30 years** | 106 | 62. 4 |
| **30-40 years** | 61 | 35. 9 |
| **More than 40** | 3 | 1. 8 |
| **Total** | 170 | 100. 0 |

Remarkable thing about Jawwal, it is being Young institution, since just 1. 8% from respondents are more than 40 year,. This results in harmonize with, Robb Mattison, GRAPA, revenue assurance (Mattison, 2009), he said in general, people involved in revenue assurance have been working from three to ten years, meaning that the majority of revenue assurance professionals are in mid20s mid 30s age group.

## 5 . 2 Questionnaire content:

The questionnaire was provided with a covering letter explaining the purpose of the study, the way of responding, the aim of the research and the security of the information in order to encourage a high response. The questionnaire included multiple choice questions: which used widely in the questionnaire, the variety in these questions aims first to meet the research objectives, and to collect all the necessary data that can support the discussion, results and recommendations in the research.

**The sections in the questionnaire will verify the objectives in this research related to fraud management and fraud detection at Jawwal Company as the following:**

**First field**: Primary information consist from 4 questions

**Second field**: Gaps-motivations-cracks leading to fraud consist from 36 questions

And all questions related to ordinal data and each question consists from four categories.

**Pilot Study:**

A pilot study for the questionnaire was conducted before collecting the results of the sample. It provides a trial run for the questionnaire, which involves testing the wordings of question, identifying ambiguous questions, testing the techniques that used to collect data, and measuring the effectiveness of standard invitation to respondents.

**Validity of the Research:**

We can define the validity of an instrument as a determination of the extent to which the instrument actually reflects the abstract construct being examined. "Validity refers to the degree to which an instrument measures what it is supposed to be measuring". High validity is the absence of systematic errors in the measuring instrument. When an instrument is valid; it truly reflects the concept it is supposed to measure. Achieving good validity required the care in the research design and sample selection. The amended questionnaire was by the supervisor and three expertises in the tendering and bidding environments to evaluate the procedure of questions and the method of analyzing the results. The expertise agreed that the questionnaire was valid and suitable enough to measure the purpose that the questionnaire designed for.

## 5 . 3 Content Validity of the Questionnaire

Content validity test was conducted by consulting two groups of experts. The first was requested to evaluate and identify whether the questions agreed with the scope of the items and the extent to which these items reflect the concept of the research problem. The other was requested to evaluate that the instrument used is valid statistically and that the questionnaire was designed well enough to provide relations and tests between variables. The two groups of experts did agree that the questionnaire was valid and suitable enough to measure the concept of interest with some amendments.

## 5 . 4 Statistical Validity of the Questionnaire

To insure the validity of the questionnaire, two statistical tests were applied. The first test is Criterion-related validity test (spearman test) which measures the correlation coefficient between each item in the field and the whole field. The second test is structure validity test (spearman test) that used to test the validity of the questionnaire structure by testing the validity of each field and the validity of the whole questionnaire. It measures the correlation coefficient between one filed and all the fields of the questionnaire that have the same level of similar scale.

**Criterion Related Validity:**

**- Internal consistency:**

Internal consistency of the questionnaire is measured by a scouting sample, which consisted of thirty questionnaires, through measuring the correlation coefficients between each paragraph in one field and the whole filed. Tables No. (12) Below shows the correlation coefficient and p-value for each field items. As show in the table the p- Values are less than 0.05 or 0.01, so the correlation coefficients of this field are significant at α=0.01 or α=0.05, so it can be said that the paragraphs of this field are consistent and valid to be measure what it was set for.

***Table (12): The correlation coefficient between each paragraph in the field and the whole field (Fraud detection on net of JAWWAL companies)***

| No. | question | Pearson coefficient | p-value |
|---|---|---|---|
| 1 | The importance of anti fraud section | 0. 677 | 0. 000 |
| 2 | The most important step to stop fraud | 0. 621 | 0. 000 |
| 3 | The Fraud effects | 0. 545 | 0. 002 |
| 4 | The main impact of fraud attacks: | 0. 685 | 0. 000 |
| 5 | How most fraud cases are discovered | 0. 517 | 0. 003 |
| 6 | The bad debit resulting from fraud | 0. 565 | 0. 001 |
| 7 | The subscribers fraud motivation | 0. 737 | 0. 000 |
| 8 | Fraud awareness writhen Jawwal company | 0. 526 | 0. 003 |
| 9 | Jawwal employee | 0. 498 | 0. 005 |
| 10 | The sales personnel | 0. 600 | 0. 000 |

| No. | question | Pearson coefficient | p-value |
|---|---|---|---|
| 11 | The number of fraud cases which are discovered and detected | 0. 700 | 0. 000 |
| 12 | The insolvent customer differ from fraudulent customer: | 0. 524 | 0. 003 |
| 13 | The fraudulent customer | 0. 401 | 0. 028 |
| 14 | How the customer consider fraudulent | 0. 480 | 0. 007 |
| 15 | The current criteria to identify the fraudulent | 0. 397 | 0. 030 |
| 16 | How the anti fraud employee can identify the fraudulent customer | 0. 585 | 0. 001 |
| 17 | How The sales target is consider a window of fraud attacks | 0. 406 | 0. 026 |
| 18 | How The dealers are consider a window of fraud attacks | 0. 641 | 0. 000 |
| 19 | The policies and procedures | 0. 604 | 0. 000 |
| 20 | The accelerate modifying of policies and procedures | 0. 504 | 0. 005 |
| 21 | Promotions and campaigns | 0. 445 | 0. 014 |
| 22 | Current fraud detection tools | 0. 303 | 0. 104 |
| 23 | The fraud management system | 0. 412 | 0. 024 |
| 24 | Billing reports | 0. 364 | 0. 048 |
| 25 | The black list window | 0. 537 | 0. 002 |
| 26 | The information regard fraud attacks from recourse like(complaints-call center-sales-provisioning) | 0. 516 | 0. 003 |
| 27 | The documents in new superscriptions and agreements | 0. 685 | 0. 000 |
| 28 | The services activated by default | 0. 593 | 0. 001 |
| 29 | The guarantee policy | 0. 422 | 0. 020 |
| 30 | The pricing policy | 0. 721 | 0. 000 |
| 31 | The most service consider vulnerable to the fraud attacks | 0. 542 | 0. 002 |
| 32 | The increasing number of fraud attacks in Gaza region | 0. 431 | 0. 017 |
| 33 | The increasing number of fraud attacks in corporate department | 0. 575 | 0. 001 |
| 34 | The most efficient way to detect fraud | 0. 742 | 0. 000 |
| 35 | Collaborative efforts between some destinations like (epaltel-banks-) : | 0. 394 | 0. 031 |

## Reliability of the Research:

Reliability of an instrument is the degree of consistency with which it measures the attribute it is supposed to be measuring. The test is repeated to the same sample of people on two occasions and then compares the scores obtained by computing a reliability coefficient. For the most purposes reliability coefficient above 0. 7 are considered satisfactory. Period of two weeks to a month is recommended between two tests Due to complicated conditions that the contractors is facing at the time being, it was too difficult to ask them to responds to our questionnaire twice within short period. The statistician's explained that, overcoming the distribution of the questionnaire twice to measure the reliability can be achieved by using Kronpakh Alph coefficient and Half Split Method through the SPSS software.

## Half Split Method:

This method depends on finding Pearson correlation coefficient between the means of odd rank questions and even rank questions of each field of the questionnaire. Then, correcting the Pearson correlation coefficients can be done by using Spearman Brown correlation coefficient of correction. The corrected correlation coefficient (consistency coefficient) is computed according to the following equation:

Consistency coefficient = 2r/(r+1), where r is the Pearson correlation coefficient. The normal range of corrected correlation coefficient 2r/(r+1) is between 0.0 and +1.0 As shown in Table (7), and the general reliability for all items equal 0.8524, and the significant (α ) is less than 0.05 so all the corrected correlation coefficients are significance at α = 0.05. It can be said that according to the Half Split method, the dispute causes group are reliable.

***Table (13): Split-Half Coefficient method***

| Section | no, of question | person-correlation | Spearman-Brown Coefficient | Sig. (2-Tailed) |
|---|---|---|---|---|
| Gaps-motivations-cracks leading to fraud: | 36 | 0. 7428 | 0. 8524 | 0. 000 |

## Cronbach’s Coefficient Alpha:

This method is used to measure the reliability of the questionnaire between each field and the mean of the whole fields of the questionnaire. The normal range of Cronbach’s coefficient alpha value between 0.0 and +1.0, and the higher values reflects a higher degree of internal consistency. As shown in Table (8) the Cronbach’s coefficient alpha was calculated for all items, and the general reliability for all items equal 0.8792. Which is considered high; the result ensures the reliability of the questionnaire.

***Table (14): Reliability Cronbach's Alpha***

| section | NO. of question | Cronbach's Alpha |
|---|---|---|
| Gaps-motivations-cracks leading to fraud: | 36 | 0. 8792 |

## Statistical Manipulation:

To achieve the research goal, researcher used the statistical package for the Social Science (SPSS) for Manipulating and analyzing the data.

## Statistical Methods are as Follows:

a. Frequencies and Percentile.

b. Alpha - Cronbach Test for measuring reliability of the items of the questionnaires.

c. Person correlation coefficients for measuring validity of the items of the questionnaires.

d. Spearman –Brown Coefficient.

e. Chi square test.

# CHAPTER [6]

# DATEA ANALYSIS AND DISCUSTION

## Gaps-motivations-cracks leading to fraud:

### 1. The importance of anti fraud section:

***Table (15): The importance of anti fraud section***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Very important | 146 | 85. 9 |
| Important | 24 | 14. 1 |
| Neutral | 0 | 0. 0 |
| Not important | 0 | 0. 0 |
| **Total** | 170 | 100. 0 |

a. 86% from the respondents answered that the anti fraud section is very important, this results agreed with Johen H. van Heerden, (heerden 2005), he said the mobile telecommunications industry suffers major losses due to fraud, because of direct impact of fraud on the bottom line of networks operator, the prevention and detection of fraud become apriority.

b. What Namibias Minister of Works, Transport and Communication Joël Kaapanda said, strengthen the results in the table 15, in conference held the auspices of the Forum for International Irregular Network Access (FIINA) take place in Namibia, 2005(Namibia Economist, 2005), he said" fraud management and revenue assurance are important components of all companies and all societies as stakeholders, and network security experts and fraud managers, are an integral part of effective management of telecommunications companies today. Fraud is a global problem that threatens the profits of telecommunications companies around the world. Though accurate fraud figures are nearly impossible to pin down, FIINA itself estimates a total figure of around 56 billion Euros of losses worldwide due to telecom fraud and security-related problems. It is thus clear that telecommunications fraud is one of the fastest growing industries in the world and one of the most profitable of illegal activities".

2. **The most important step to stop fraud is:**

***Table (16): The most important step to stop fraud***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Subscription | 88 | 51. 8 |
| Activation | 33 | 19. 4 |
| Fraud prevention | 27 | 15. 9 |
| Fraud detection | 22 | 12. 9 |
| **Total** | 170 | 100. 0 |

a. Half of the respondents agreed that the activations step is the most important step to stop fraud, since the subscription for the service considering the window for the fraudsters to attack the operator. At Jawwal the subscription fraud was the most popular type, before Jawwal creation of the black list program, which considered as database contains all the disconnected customers, and did not pay there invoices, whatever the account type is individual or corporate, clarifying customer details, …. (Name, number, addresses, activation date, the unpaid amounts, the returned cheeks, and the deactivation date). In addition to the formal documents the subscription form required, such as (ID, clear and stabile address, security deposit, signature), all of these are Jawwal precautions regard the subscription fraud. These precautions deserved the attention Jawwal pays for this type of fraud, and this agreed with the conference survey results which were held in Singapore (2007), the conference was about telecom fraud and fraud prevention, 76. 5%agreed that the subscription fraud is the most fraud type currently detected, from seventeenth conference attendance from Europe, Middle East, and south-east Asia operators (CR-X, 2007).

b. In deticta, white paper (Deticta, 2006), detecting telecom subscription fraud, they said, subscription fraud is characterized by fraudsters using false identities in order to purchase a service from the operator for which they have no intention to pay. One of the major issues in detection subscription fraud is in difficulty in differentiating it from simple bad debt, when genuine customers are unable to pay; some estimate that nearly 30-35% of all bad debts are actually subscription fraud.

c. An 2006 survey for the Home Office (The Home Office is the lead government department for immigration and passports, drugs policy, crime, counter-terrorism and police) suggests that over 1. 7 billion of identity fraud take place annually in the UK, 372 million in the telecom operator sector alone, based on TUFF estimates that identity fraud /subscription fraud could account for 40% of all telecom fraud in the UK (Deticta, 2006).

d. It is estimated that 70% of fraud losses rates to subscription fraud which is over728 billion a year (78 million dollars a day), (Robert and Dabija ,2009)

### 3. The fraud affects at:

***Table (17): The Fraud affect***

| | Frequency | Valid Percent |
|---|---|---|
| Revenue and losses | 24 | 14. 1 |
| Reputation | 13 | 7. 6 |
| Service quality | 1 | . 6 |
| All of the above | 132 | 77. 6 |
| **Total** | 170 | 100. 0 |

a. 77% from the respondents agreed that fraud affects do not include only the losses from unpaid invoice; they agreed also that fraud might lead to optional loss of new and existing customers, as well as bad publicity, the above results agreed with what deticta white paper, titled by detecting telecom subscription fraud (deticta, 2006), they said about the impact of fraud on mobile operator and their customers, the impact of fraud is far-reaching and can affect all parts of mobile operator's business. Not only is there an obvious financial impact but there can also be serious damage to the operator's brand, customer relationship and shareholder confidence. Furthermore, network operations can be disrupted and legal and regulatory requirements can be breaches.

b. The financial losses due to fraud can be built up in several ways. Firstly there is the direct revenue lost when fraudster make use of mobile voice and data without baying commonly compounded by having the stolen services re-sold to other subscriptions. On the top of which is the direct cost of fraud, when the operator is left to pay for fraudulently acquired service and cannot defray the cost. Common trick for fraudster is to direct calls to their own premium rate service, by tricking mobile users to call their premium rate number. The mobile operator ends up paying commission to the premium rate service owner but is not able to recover the cost.

c. To add insult to injury, fraud can result in Mobil operators breaching legal and regulatory requirements, which carries the risks of bad publicity and fines, on a wider front, bad publicity related to fraud can damage the operator brand, breach corporate social responsibility policies, depress shareholders confidence and affect stock market performance, fraud can also cause network traffic issues and disrupt the smooth running of the network potentially affecting the quality of the service available to legitimate users.

d. Finally fraud is increasingly becoming a customer relations issue; it can adversely affect the service quality and directly affect customer bills, both of which can lead to disputes and possible legal actions. Since customers are increasingly aware and concerned about Mobil data security and privacy, inadequate fraud protection can therefore results in damages customer reactions and will most likely causes customers to churn to networks perceived to be more secure.

**4. The main impact of fraud attacks consider:**

***Table (18): The main impact of fraud attacks***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| A lot and imposes financial losses | 22 | 12. 9 |
| Few but serious | 65 | 38. 2 |
| Moderate | 42 | 24. 7 |
| Neutral | 41 | 24. 1 |
| **Total** | 170 | 100. 0 |

38% from the respondents considers the fraud losses few but serious, meanwhile the rest of the sample consider it normal or moderate losses, no one really know how much fraud is costing the industry, they can estimate the cost because Jawwal is reluctant to admit to fraud or are not actively looking for fraudulent accounts in the bad debt.

## 5. Most fraud cases are discovered by:

***Table (19): How fraud cases are discovered***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Sales person accuracy' | 39 | 22. 9 |
| Fraud management system | 80 | 47. 1 |
| Billing reports | 22 | 12. 9 |
| By chance | 29 | 17. 1 |
| **Total** | **170** | **100. 0** |

a. 47% from the respondents believe that most of the fraud cases and acts are discovered by the fraud management system, and 23% believe that it is the sales person accuracy, in fact the reality is most fraud cases are discovered by high usage reports (billing reports) and by chance, and the results above indicates that there is a little awareness of anti fraud sections functions and programs used to detect fraud among the employees.

b. Jawwal FMS is ill program and the functions of anti fraud section did not rely on it as the main tool to detect fraud.

c. The above facts agreed with what GRAPA, Global revenue assurance professional association, white paper presents by Ade Banjako, about fraud management methodology in developing countries (Banjako, 2009), he said the Startups tend to rely on high usage alerts based on call types, value, duration or even credit limits. This function often has close similarities to credit control and it is important to clearly define the role of the fraud team so that they can concentrate on managing fraud.

### 6. The bad debit resulting from fraud is:

*Table (20): The bad debit resulting from fraud*

| | Frequency | Valid Percent |
|---|---|---|
| Normal | 46 | 27. 1 |
| Worrisome | 9 | 5. 3 |
| Requiring more auditing on anti fraud | 99 | 58. 2 |
| Consider huge and should be taken into consideration | 16 | 9. 4 |
| **Total** | 170 | 100. 0 |

There is an important difference between bad debts and fraud, bad debts concerns people with occasional difficulties in paying their invoices, this happens only once or twice per person, if the subscriber really can't pay, he or she will most probably be suspended and denied to open a new subscription in the future, but fraud always include lie and there is no intention to pay for the used service. 58% from the respondents said that more auditing in anti fraud activities should be done, since bad debt is may hide in the subscription fraud. This is agreed with Hoath as sited in the study of Abidogun (Abidogun,2005) that " subscription fraud can be committed upon fixed line and mobile telephone, and it is usually difficult to distinguish from bad debt, particularly if the fraud for personal usage, both subscription fraud and bad debts are major problems to telecoms in developing and third world countries".

### 7. The subscribers' fraud motivations are:

*Table (21): The subscriber's fraud motivation*

| | Frequency | Valid Percent |
|---|---|---|
| Bad experience | 8 | 4. 7 |
| The subscriber inelegance and innovation | 29 | 17. 1 |
| Monetary value | 35 | 20. 6 |
| All of the above | 98 | 57. 6 |
| **Total** | 170 | 100. 0 |

57% from the respondents insure that fraudster's motivations to commit fraud attacks are bad experience, the subscriber inelegances and innovation, and also monetary value, these findings agreed what previous studies clarified.

**Greed:**

The primary motivation which causes offenders to steal mobile telephones and use them to obtain services without incurring a charge to themselves is greed. Offenders may simply seek to exploit the opportunities provided by new forms of telecommunications technology to obtain calls for free (although, of course, the calls are in fact only free to the offender and the legitimate subscriber has to pay unless some other arrangement can be negotiated with the service provider). Some offenders have established lucrative businesses of dealing in stolen equipment and services Delaney (as cited in smith).

**Curiosity:**

If one examines the history of theft of telecommunications services one important factor emerges which distinguishes these crimes from traditional property offences. This is the purpose for which the illegal conducts carried out. The very early cases of improper use of fixed-wire telephone services were often undertaken not for profit but out of curiosity. Sheer interest in how systems work and the challenge of defeating security measures provides a powerful incentive which drove many individuals to commit offences against telecommunications systems. Clough , Mungo and Parker (as cited in smith).

The same motivation can be seen to apply in the case of offenders who steal mobile telephone services.

The sophisticated technological procedures needed to scan security numbers and to produce counterfeit telephones obviously creates a keen challenge to technologically-minded individuals with a desire to break the law. Traditional deterrence-based sanctions which operate in respect of offenders whose motivations are primarily financial, may, therefore be inappropriate when dealing with individuals who are not intent on making a profit from their enterprise.

**Envy:**

In a time when new technological developments are taking place, particularly those involving attractive consumer goods such as mobile telephones which are highly publicized, there is a possibility that new social divisions could emerge based upon access to and familiarity with the new technologies. People without access to mobile telephones, for example, may feel isolated and deprived and a new environment conducive to criminality may be created in which theft of telephones and telecommunications services will become a major social problem.

**Need:**

Mobile telephones have become a readily saleable commodity on the black market making them attractive to individuals who need to obtain funds by criminal conduct. In a plea made in mitigation of sentence in the Melbourne Magistrates' Court recently, a mobile telephone thief was described as being unemployed and trying to treat a drinking problem Butcher(as cited in smith). In another case heard before the same court in which the offender had stolen one hundred mobile telephones from motor vehicles, the offender told police that he needed money to keep a roof over his head and to pay for food ,Adams (as cited in smith).

In the United States, the proliferation of illegal mobile telephones was such that organized groups of criminals became involved in selling telephone services to those who were unable to obtain legitimate access to services such as the indigent and illegal immigrants. In New York City, one such group, the 'Orchard Street Finger Hackers' became notorious. This group of offenders, who came out of the cocaine-dealing sub-culture, sold stolen long-distance telephone services in various unsavory neighborhoods to a captive clientele of illegal immigrants who were desperate to call home ,Sterling (as cited in smith).

### 8. Fraud awareness writhen Jawwal company:

***Table (22): Fraud awareness writhen Jawwal Company***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Great degree of awareness an all company levels | 40 | 23. 5 |
| There is partial awareness and some particulars sections and department | 91 | 53. 5 |
| Insignificant awareness | 36 | 21. 2 |
| Lacking of awareness | 3 | 1. 8 |
| **Total** | 170 | 100. 0 |

9. **Jawwal employees are:**

***Table (23): Jawwal employee***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Qualified enough to deal with fraud problem and fraudulent | 32 | 18. 8 |
| Qualified but needs training | 77 | 45. 3 |
| Not qualified | 51 | 30. 0 |
| No need for fraud prevention and detection qualifications for most employees | 10 | 5. 9 |
| **Total** | 170 | 100. 0 |

a. Fraud awareness training is the consumer or professional's key to preventing, detecting and dealing with instances of fraud. For many employers, fraud awareness is a valuable asset in employees because employees who detect fraud can save the company up to billions of dollars. 53% from the respondents answers were that there is partial awareness in some particulars sections and department, this answer clarify that the anti fraud employees and employees on related sections such as revenue assurance and risk operations are the sections that had some deep knowledge regard the fraud threats against the company, on the other hand employees in other sections such as engineering, marketing, and even sales had less knowledge regard the fraud issues.

b. In the question related to Jawwal employees qualifications and training, 45% from respondents were that the employees are qualified but needs training, these results agreed with what Delotte and Touch white paper, titled by Fraud Detection and prevention: are you doing enough (Delotte and Touch, 2006), when they asked what particular activity would most benefit your organization in terms of reducing fraud risked, 37.6% answered that fraud awareness training throughout the organization, and this is was the highest percent, on the other hand, in Indian fraud survey report in 2006 (KPMG, 2006), the majority of the respondent had not been imparted any form of training or awareness program, only 35% percent of the respondent agreed that they had received some training on how to implement anti fraud procedures and controls and out of these people 63% indicated that these programs were conducted once a year.

c. Another survey conducted by ERNST and YOUNG "fraud risk in emerging markets (ERNST and YOUNG, 2006), the results indicates that all of companies surveyed, alarmingly 72% don't provide their employees with training to understand and implement the organization's anti fraud policy

d. To achieve the objective of detecting fraud, it is important that anti fraud stance become a part of the organizations culture, and formal training and awareness programmers are held periodically to communicate and re-emphasize the importance of appropriate anti fraud mechanisms.

**10. The sales personnel are:**

***Table (24): The sales personnel***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Qualified and having sufficient knowledge of fraud problem | 58 | 34. 1 |
| Qualified but the priority is for sales target only | 55 | 32. 4 |
| Not qualified | 47 | 27. 6 |
| Flexible with fraud cases in negative way | 10 | 5. 9 |
| **Total** | **170** | **100. 0** |

34% from the respondents agreed that the sales personnel are qualified and having sufficient knowledge of fraud problem, but since that 56% from the respondents were from sales then this is expected answer, but the logical answer from the researcher point view is that sales personal are qualified but the priority is for sales target only. According to a recently released study conducted by Redshift Research at the request of telecoms supplier Denovo as sited in softpedia (sofpedia, 2008), businesses turn a blind eye to telecom related security issues, most companies believe that this type of fraud will not impact them in a significant manner and prefer to focus their attention on other security issues, such as data loss and sales penetration.

## 11. The number of fraud cases which are discovered and detected are:

*Table (25): The numbers of fraud cases which are discovered and detected*

| | Frequency | Valid Percent |
|---|---|---|
| Rare | 17 | 10. 0 |
| Few and refer to the anti fraud efficiency | 61 | 35. 9 |
| Moderate and refer to improving anti fraud | 86 | 50. 6 |
| Numerous and refer to the need for more efficient anti fraud tools | 6 | 3. 5 |
| **Total** | 170 | 100. 0 |

50% from the respondent agreed that the number of fraud case which are detected are not dangers, it is moderate, and that is required improving of the current anti fraud tools, and whatever the efficiency of anti fraud tools we cannot eliminate fraud permanently since the fraudsters are adaptive and will keep attacking the operators.

## 12. The insolvent customer differs from fraudulent customer in:

*Table (26): How the insolvent customer differs from fraudulent customer?*

| | Frequency | Valid Percent |
|---|---|---|
| Intention to not defraud ate | 34 | 20. 0 |
| Commitment | 8 | 4. 7 |
| Possibility to pay the due amounts | 15 | 8. 8 |
| All of the above | 113 | 66. 5 |
| **Total** | **170** | **100. 0** |

## 13. The fraudulent customer:

*Table (27): The fraudulent customer*

| | Frequency | Valid Percent |
|---|---|---|
| Had the intention to defraud ate | 40 | 23. 5 |
| Had Bad experience with the company | 7 | 4. 1 |
| Utilize the system gaps | 30 | 17. 6 |
| All of the above | 93 | 54. 7 |
| **Total** | **170** | **100. 0** |

## 14. The customer consider fraudulent if:

*Table (28): How the customer consider fraudulent?*

| | Frequency | Valid Percent |
|---|---|---|
| Having the intention to defraud ate | 13 | 7. 6 |
| Illegally using of company service | 18 | 10. 6 |
| Used false documents | 11 | 6. 5 |
| All of the above | 128 | 75. 3 |
| **Total** | **170** | **100. 0** |

66% from the respondent agreed that the insolvent customer had no intention to defraud the operator, had commitment with company, and if the service permanently disconnected, there is away to collect the unpaid amounts, on the other hand the fraudulent one had intention to miss use the service, and will never pay the due amounts, also will use false documents to activate the service that what is 54% from respondents agreed with, in question (13), and also 75% from the respondents in question (14) agreed with that results, these are the main differences between the bad debtors and fraudulent, the intention is the main criteria to distinguish them, another point should be mentioned, that Jawwal did not differentiate between the collectable amounts and uncollectable amounts, since the collectable one are bad debit, meanwhile the uncollectable on is fraud losses.

## 15. The current criteria to identify the fraudulent are:

***Table (29): The current criteria to identify the fraudulent***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Efficient and leads to discover all of the fraud customers | 27 | 15. 9 |
| Efficient but it's being relativity makes the fraud attacks possible | 76 | 44. 7 |
| Needs to be more effective | 57 | 33. 5 |
| Not efficient and there is need for a new criteria | 10 | 5. 9 |
| **Total** | **170** | **100. 0** |

a. 44.7% from the respondents agreed that the current criteria to identify the fraudulent are efficient but it is being relatively makes the fraud attacks possible, also 33. 5% agreed that there is need for these tools to be more effective, the total 78% from the respondents indicate that the current tools are not effective and did not protect the company in efficient manner, for examples, one of internal business rule(policies) " if the customer usage is more than 50% of his maximum paid invoice, and he subscribe for the service for more than 2 years, no action should be taken regard him, but if the customer is newly activated, and his first invoice more than his security deposit (800 NIS) action should be taken to disconnect the service "From researcher point view" these are ill policies and procedure, and for sure having gap to defraud ate the system, also the they are incomprehensive.

b. The previous results agreed with Indian fraud survey report (KPMG, 2006), 25% of the respondents indicated that their current anti fraud procedure and controls are not adequate and 33% said they are cannot say that the current anti fraud procedures and control are adequate. In general it is imperative for company to establish adequate anti fraud control.

## 16. The anti fraud employee can identify the fraudulent customer by:

***Table (30): How fraudulent customer can be identified***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| The sudden change in his usage (calls /services) | 17 | 10. 0 |
| The kind of service the customer requests | 15 | 8. 8 |
| The number of lines requested | 13 | 7. 6 |
| All of the above | 125 | 73. 5 |
| **Total** | **170** | **100. 0** |

73% from the respondents agreed that the customer suspects to be fraudulent if there is sudden increase in his invoice amounts, if some critical services requested such as the international dialing access, and international roaming access, also if the customer request additional lines in short periods. All of these are indicators which helping the anti fraud analyst to shade off suspecting fraud customers.

## 17. The sales target is consider a window of fraud attacks through:

***Table (31): The sales target is consider a window of fraud attacks***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Sales person concentration on acquiring the target not the service quality | 43 | 25. 3 |
| Working under pressure | 31 | 18. 2 |
| Carelessness to stop some of inaccurate superscription | 12 | 7. 1 |
| All of the above | 84 | 49. 4 |
| **Total** | 170 | 100. 0 |

49% from the respondents agreed that sales person consider window of fraud attacks, when they are concentrating on acquiring the sales target, instead of the service quality, for example carelessness to stop some fraudulent suspects of services requests, ignorance of clarifying to the new customers the high roaming tariffs and the prices of premium sms, in addition working under pressure, lead to the same result for not concentrating on expected fraud attacks.

## 18. The dealers are consider a window of fraud attacks through :

***Table (32): The dealers are consider a window of fraud attacks***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Having separate aims | 26 | 15. 3 |
| Insufficient knowledge about fraud problems | 24 | 14. 1 |
| Absence of procedures and rules that focus on fraud problem | 25 | 14. 7 |
| All the above | 95 | 55. 9 |
| **Total** | 170 | 100. 0 |

a. 56% from respondents agreed that dealers are consider a window of fraud attacks, because the conflict of interest between the dealers (they are looking for the commotions mainly) and the company interest which looks for market penetration and profit. Also the workers within the reseller and dealer outlets had limited knowledge about the fraud problem and attack, another issue is the business roles Jawwal established did not control the relation with the dealer and distributor in the light of fraud problem, also the internal anti fraud polices, did not shad of these point clearly.

b. An important issue should mentioned, is the fraudulent choose to get the access to the operator via dealer, they choose the easiest way because they had the information about the weakness dealers had particularly in fraud subject, about Jawwal dealers are considered window for subscription fraud particularly

c. The above result agreed with study of Stephen Brown, " telecommunication fraud management (Brown, 2005), the study said that the resellers' (wholesaler) may represents risk, therefore, the need to effectively manage relationship is absolutely necessary and requires appropriate action with commercial dealers:

    i. Interconnect agreements should address fraud.

    ii. Corporate with partners on identifying frauds.

    iii. Use similar fraud prevention technology such as authentication.

## 19. The policies and procedures are:

***Table (33): The policies and procedures***

| | Frequency | Valid Percent |
|---|---|---|
| Clear about fraud problem | 47 | 27. 6 |
| Unclear and there gabs | 81 | 47. 6 |
| Unclear and incomprehensive | 31 | 18. 2 |
| Unclear and need to be modified | 11 | 6. 5 |
| **Total** | **170** | **100. 0** |

a. Since business's internal controls are policies and procedures designed to reduce opportunities for fraud, 47% from the respondent agreed that the policies and procedures are unclear about the fraud and there gabs, the result trend in the above table is toward approving that the policies and procedures are week (contains gabs, and incomprehensive), Some interesting results are in 9th fraud survey, conducted by ERNST and YOUNG "fraud risk in emerging markets", in (ERNST and YOUNG, 2006), the report is a result of interviewing and listing to over 500 corporate leaders, including chief executive officers, chief financial officers, chief risk officers, internal audit directorate, and business unit directorates, they represent many of the world organization, Since the internal control, is about policies and procedures.

b. Robust internal control remain the first line of defense against fraud for all companies in all markets, but anti fraud controls are not always integrated under an-fraud program, or separately monitored for operating effectiveness.

c. Internal control are still the most likely factor to prevent and detect fraud, nearly 90% the respondents believed control was sufficient within their organization to identify and investigate fraud promptly, however, over 40% of respondents are without formal or documented anti fraud policy.

d. The results indicate that internal control is just one element of a company's comprehensive anti fraud effort; you cannot control fraud out of existence.

e. Strong internal control environment should also include formal anti fraud policy to maximize it is effectiveness.

### 20. The accelerate modifying of policies and procedures is:

*Table (34): The accelerate modifying of policies and procedures*

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Useful and serve work | 41 | 24. 1 |
| Useful but need to be more slow | 52 | 30. 6 |
| Useful but separate the employee attention | 66 | 38. 8 |
| Un useful and not serve the work | 11 | 6. 5 |
| **Total** | **170** | **100. 0** |

38% from the respondents agreed that the accelerate modifying of policies and procedures is useful but separate the employee attention, from the researcher point of view it separate the attention for sales employees in particular, and under the work presser some important update will be missed by the employees or did not consider, it is very important for the sales operation and the top management to set the circulated note in comprehensive way and then popularize it.

### 21. Promotions and campaigns are:

*Table (35): Promotions and campaigns*

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Comprehensive and accurate | 30 | 17. 6 |
| Skillful but contains gaps to defraud company | 76 | 44. 7 |
| not accurate and there is gaps to defraud ate the company | 35 | 20. 6 |
| They are not consider window to defraud ate | 29 | 17. 1 |
| **Total** | **170** | **100. 0** |

44.7% from the respondents agreed that the Promotions and campaigns when lunching new product and services, are skillful but contains gaps to defraud the company, the above results strengthen the need for fraud risks assessments with new products and services, since each product and service in the market represents a potential new opportunity for fraudulent attack. Pressure to launch new services to gain competitive advantage often results in little attention to security or fraud initiatives. This risk is compounded when these services are offered by new operators or in highly competitive markets, key aspect of fraud management role is to be an integral part of the new product and service development process, the fraud team needs to ensure they can determine the required points of control, measurement, and monitoring to ensure appropriate prevention initiatives are in place (Thameem).

### 22. Current fraud detection tools are:

***Table (36): Current fraud detection tools***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Comprehensive and reliable | 27 | 15. 9 |
| Reliable but not comprehensive | 72 | 42. 4 |
| A need to more efficient tools there | 36 | 21. 2 |
| one efficient tool will be more accurate | 35 | 20. 6 |
| **Total** | **170** | **100. 0** |

42% from the respondent agreed that the current fraud tools are reliable but not comprehensive, to light up this point Jawwal current anti fraud tools are: the fraud management system, and it is ill program and the company in process to purchase a new program, the HUR, which consider the main tool to discover the high usage customers these are the two main tools. These findings agreed with what stated in the comments in question 19.

### 23. The fraud management system is:

***Table (37): The fraud management system***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Comprehensive and reliable | 32 | 18. 8 |
| Reliable but not comprehensive | 55 | 32. 4 |
| Needs update and modification | 65 | 38. 2 |
| Jawwal needs to employ new program | 18 | 10. 6 |
| **Total** | **170** | **100. 0** |

38% from the respondents agreed that the current FMS, needs update and modifications, this means that the program is not efficient tool to detect fraud, the program name is Secure Wave™ is an ad-hoc solution that allows users to set intuitive language based rules to monitor fraud conditions in the network. Through a self-learning profiling engine, the system generates alerts to identify abnormal behavior, which in turn can be indicative of fraud. The Case Tracking System becomes the backbone of the company fraud management center. It automatically quantifies averted loss by fraud center agent derived from rating tables. The system then stores and records all fraudulent cases, making the information available for reports based on account managers, agents, customers, case categories, and summaries.

But the current status for the program is there are gabs and Jawwal Company decided to deleted the users access for it, the company in process to purchase new system.

The above results agrees with (Commverg solution, 2010), Most operators have a Fraud Management System (FMS) already in place but are still unable to tackle fraud losses due to inflexibility and too much dependency on the vendor preventing the operator to quickly adapt to constantly changing fraudulent and legitimate behaviors. It is crucial to adapt the latest FMS detection techniques which are more capable of stopping emerging fraud types, enabling an increased efficiency in the detection processes. FMS should incorporate the latest detection technologies that are capable of evolving and quickly apprehending to those changes.

### 24. Billing reports are:

***Table (38): Billing reports***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Main tool to fraud detection | 30 | 17. 6 |
| Supportive tool to fraud detection | 80 | 47. 1 |
| Supportive but not useful | 48 | 28. 2 |
| Not reliable tool to depend on to detect fraud | 12 | 7. 1 |
| **Total** | **170** | **100. 0** |

a. 47% from the respondents agreed that HUR are Supportive tool to fraud detection, but from the researcher point of view, this is untrue, since the HUR, considered now the main tool to in classifying the high usage customers, then sorting the customer according to cretin consideration such as (activation date, total paid amount, maximum paid invoice, unbilled charges, the usage to some services such as international dialing service and international roaming access), that because as we stated in the comments about the previous table, that the FMS is ill program. And the results came in this way because of lack awareness about the anti fraud functions.

b. Another point should be highlighted, is the lack of efficiency these reports had, they contained huge amount of numbers, and the treated manually, so it is consuming a lot of time.

### 25. The black list window is:

***Table (39): The black list window***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Comprehensive data base to discover the black listed customers | 49 | 28. 8 |
| Comprehensive data base but not sufficient to discover all the black listed customers | 51 | 30. 0 |
| Needs modification | 67 | 39. 4 |
| Not efficient toll to discover the black listed customers | 3 | 1. 8 |
| **Total** | **170** | **100. 0** |

a. 39. 5% from the respondents agreed that the black list window is need modification, and 30% agreed that this window is not sufficient, in brief its window of data base, contend all the permanently disconnected accounts, contains details about the account such as name, ID, Jawwal number, address, outstanding, deactivation date, in case of corporate accounts, the authorized signature name is mentioned, and another window for returned check, this window is the back bone of the new activation units, since all the new accounts are audited on this programs, it is minimize the subscription fraud mainly.

b. What Jawwal implements agreed with what preasidum work shop clarifying (Robert and dabija, 2009), workshop indicates that many operator implement black list of known fraudulent details, to prevent new applications from being activated using known fraudulent details,

**26. The information regard fraud attacks from recourse like (complaints-call center-sales-provisioning) are:**

***Table (40): The information regard fraud attacks from recourse like (complaints-call center-sales-provisioning)***

| | Frequency | Valid Percent |
|---|---|---|
| Efficient source to discover the fraud cases | 56 | 32. 9 |
| Efficient source and it is roll needs to more active | 52 | 30. 6 |
| Subordinate roll | 57 | 33. 5 |
| Inefficient roll | 5 | 2. 9 |
| **Total** | **170** | **100. 0** |

Respondent answers indicates that these channels are vital source for information about the fraud cases and their roll should be activated, IUCN report (IUCN, 2008), agreed with the above results, they said some frauds arise because lake of proper internal control policies and procedures. Others frauds may be the result of failures to follow proper control procedures, carelessness in carrying out checks, inadequate separation of duties of staff or management override of internal controls.

**27. The documents in new superscriptions and agreements are:**

***Table (41): The documents in new superscriptions and agreements***

| | Frequency | Valid Percent |
|---|---|---|
| Comprehensive | 53 | 31. 2 |
| Not comprehensive | 68 | 40. 0 |
| Not efficient | 14 | 8. 2 |
| Needs to be more strict | 35 | 20. 6 |
| **Total** | **170** | **100. 0** |

40% from the respondents agreed that the subscription form and agreements information and documents are not comprehensive.

Fake identity, and documents in subscription forms and agreements considered subscription fraud, according to result of survey conducted by CFCA (CFCA, 2009), about the global fraud losses, the losses from subscription fraud /identity theft is 22$ billion

the deticta white paper, titles fraud detecting telecom subscription fraud, ( deticta, 2006), said many gangs have found that the nature of postpaid Mobil contract make them attractive for subscription fraud. The documents are proof of identity/address like photo of identity card, passport, for address verifications, electricity /water landline telephone bill, any other acceptable documentary evidence in support the address given.

AT and T, (AT and T, 2009). White paper, express about it steps in subscriptions fraud prevention

**Policy:**

a. AT and T defined subscription fraud **as**, act of identity theft, this happen to business as well as to consumer, it is also happens when unauthorized lines are added to existing account, equipment fraud, is unauthorized equipment ordered, shipped and or charged, without the account owner's authorization.

b. According to AT and T the most important methods to prevent subscription an equipment fraud are validation and verification; validate the business in person to person or via online directory.

c. Business validation via on-site visit; to validate a business, a site visit is requested, looking for the name of the company posted on the outside of the business or posted in the location you visit.

d. Dose the observations indicate the business can support the number of line requested? If you are unable to verify the applicant's purchasing authority with the business, the applicant must provide secondary business ID before the activation can be complete.

**Business validation via online directory:**

a. Advice the business applicant the AT and T must verify some information.

b. look up the business name and phone number in online directory.

c. fined the phone number of the business and confirm the business information in the application by calling the business number listed in the directory. Ask if the business applicant works for the business and has the authority to purchase wireless service on behalf of the business, if the answer to both question is "yes" proceed as verified.

d. In all face to face transactions, all applicant must present valid original photo identification, below is a list of acceptable forms of primary identification for consumer and business account applications, Consumer IRU and Business CRU applications:

  i. Drivers license issue by state or U. S possession with name address an photograph.

  ii. ii Passport issued by U. S government.

  iii. Stat ID card issued by stat Or U. S Possession with name, address, and photograph.

  iv. A line Registration Receipt card with photo.

  v. US military ID card or draft record.

  vi. Employment authorization document issued by the US with photo.

e. If the name or address do not match, an approved form of secondary ID is required that match the account or application name and address.

f. Secondary identification, in all face to face transaction, all applicants must present valid original photo identification. Secondary ID is needed when a customer's social security number is not available or when name and address on the primary ID is not an exact match with the name and address on the account /application.

g. The secondary ID must match the first and the last name on the application or account.

h. Some example of the secondary identification:

i. Consumer's student ID badge.

ii. Business issue photo badge.

iii. utility bill (within last 60 days), with utility (gaze, electric, oil, telephone, water, cable /satellite, but not wairless) name, customer name and address matching service agreement, billing data, and bill amount.

**28. The services activated by default are:**

***Table (42): The services activated by default***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Increasing company vulnerability to fraud | 25 | 14. 7 |
| Useful and serving customer | 34 | 20. 0 |
| Need to be more strict | 50 | 29. 4 |
| It is not related to fraud attacks | 61 | 35. 9 |
| **Total** | **170** | **100. 0** |

**29. The guarantee policy is:**

***Table (43): The guarantee policy***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Suitable | 41 | 24. 1 |
| Good recovery in case the customer became fraudulent | 38 | 22. 4 |
| Suitable but need to be modified | 53 | 31. 2 |
| Unsuitable for the whole customers | 38 | 22. 4 |
| **Total** | **170** | **100. 0** |

31% from the respondents agreed that the guarantee policy is suitable but need to be modified, it may be suitable for individuals but not corporate accounts, and more regulations should be applied particularly in services such as international roaming and international dialing, Jawwal guarantee policy is the customer required to make security deposit in order to be connected or reconnected to the network. This security deposit is refundable without interest after the agreement terminated and all outstanding monies due to Jawwal have been recollected, the customer required to pay deposit to be specified by use for the ability to roam or use the phone on another GSM networks which Jawwal having agreement. This security deposit may be used to settle any outstanding debt owed to Jawwal at any time. Security deposit dose not absolve the customer from his liability to pay for the service rendered through the digital SIM card, including all the costs associated with its unauthorized use

**30. The pricing policy is:**

***Table (44): The pricing policy***

| | Frequency | Valid Percent |
|---|---|---|
| Suitable and not consider motive to defraud ate the company | 65 | 38. 2 |
| High | 21 | 12. 4 |
| Moderate | 71 | 41. 8 |
| Unsuitable and consider motive to defraud ate the company | 13 | 7. 6 |
| **Total** | **170** | **100. 0** |

**31. The most service consider vulnerable to the fraud attacks is:**

***Table (45): The most service consider vulnerable to the fraud attacks***

| | Frequency | Valid Percent |
|---|---|---|
| International roaming | 73 | 42. 9 |
| International dialing | 57 | 33. 5 |
| Sort massage service | 18 | 10. 6 |
| Wape and interne | 22 | 12. 9 |
| **Total** | **170** | **100. 0** |

a. 42% from the respondents agreed that international roaming fraud is the most service vulnerable to the fraud attacks, this results agreed with survey result conducted by KBMG, (KBMG, 2009), the results are shows that the, recovery of leakages remains a problem for most regions. About 60% of operators surveyed estimated that less than half of leakages identified were recovered.

b. More than 45% of respondents ranked prepaid accounts as the revenue stream most vulnerable to leakage. In developing markets, a majority of respondents said either roaming or value added services were the second most vulnerable, while in Europe and America postpaid was ranked second

**32. The increasing number of fraud attacks in Gaza region refers to:**

***Table (46): The increasing number of fraud attacks in Gaza region***

| | Frequency | Valid Percent |
|---|---|---|
| The bad economic conditions | 52 | 30. 6 |
| The customer innovation | 34 | 20. 0 |
| Acquiring the sales target instead to service quality | 7 | 4. 1 |
| All of the above | 77 | 45. 3 |
| **Total** | **170** | **100. 0** |

77% from the respondents agreed that the economic bad conditions, customer innovation and acquiring sales target instead of service quality, are motives to increasing the fraud attacks in Gaza region. The results agreed with study conducted by The TRMG (TRMG, 2008), Socio-economic conditions are one of the primary drivers leading to some of the major classes of fraud. However it is important to recognize that in many if not most cases those who are at the lower end of the socio-economic ladder are more likely to be exploited as a market segment by organized fraudsters than they are to commit the frauds themselves. Perhaps the most common scenario is that no one has call selling. This involves an organized fraudsters setting up a bank of fixed or mobile telephones and offering cheap calls to target group, for example and immigrant population concentrated in a small urban area. The fraudster has recognized that the combination of distance from home and lower wages creates an opportunity for him to sell illegal calls to this segment.

## 33. The increasing number of fraud attacks in corporate department refers to:

***Table (47): The increasing number of fraud attacks in corporate department***

| | Frequency | Valid Percent |
|---|---|---|
| Corporate sales policy and the absent if guarantee in most of activated lines | **29** | **17. 1** |
| Sales target | **35** | **20. 6** |
| Activating some services such as ID and IR without guarantee | **13** | **7. 6** |
| All of the above | **93** | **54. 7** |
| **Total** | **170** | **100. 0** |

## 34. The most efficient way to detect fraud is:

***Table (48): The most efficient way to detect fraud***

| | Frequency | Valid Percent |
|---|---|---|
| Centralizing the anti fraud tasks | **39** | **22. 9** |
| Establishing anti fraud section in every related department | **56** | **32. 9** |
| Expanding the current anti fraud section authorities | **53** | **31. 2** |
| Fraud can't be avoided | **22** | **12. 9** |
| **Total** | **170** | **100. 0** |

a. 32% from the respondents agreed that the most efficient way to detect fraud is in establishing anti fraud section in every related department, and this is result conflicts with results of survey conducted by Bearing Point, management and technology consultant, (Bearing point, 2008), 85% of the respondents agreed that fraud management unit is organized centrally in the enterprise, it is either composed as central unit or local independent unit, with a central component, in addition many fraud departments are closely across linked with the claims departments 56% agreed about that, this is not surprise since suspicious of fraud often rise within the claims processing function. However, almost half of all fraud investigation units are housed outside the claims function: either within a legal department (21%) or as standalone unit 23%.

b. Another findings regard the central role of anti fraud department is introduced by Financial service authority in a report, tilted by Firms high level management of fraud risk (FSA, 2006), there is unclear or inappropriate allocation of anti fraud responsibilities writhen firms, anti fraud responsibilities form an inherent part of many people's responsibilities within affirm, but accountabilities for these are not clearly defined, they may be de-priorities in favors of other business needs. An operations area, for example, may place operational efficiency above the need to pause and investigate unusual customer activity, FSA finds that it is important to embedding spiciest anti fraud responsibilities in the front line of business, with these responsibilities reflected in the job description, was seen by several major firms as a key to successful fraud mitigation. Givn the diversity of the product base, and therefore the potential fraud risk faced by major firms, the knowledge and skills within and operational the customer- facing and operational parts of the business were vital resources for identifying and mitigation fraud risk and reacting quickly and effectively to fraud threats.

c. This model was typically part of a 'hub and spoke' approach whereby support was provided to the front line by a central team whose primary responsibilities were developing and enforcing polices and standards monitoring, reporting, and highlighting threats and sharing best practice however this model was not universally followed. There were more centralized approaches where fraud responsibility was 'passed through' the business to central team, adopted in some cases for reasons such as operational efficiency, and effective exchange of information

**35. Collaborative efforts between some destinations like (epaltel-banks-) are:**

***Table (49): Collaborative efforts between some destinations like (epaltel-banks)***

| | **Frequency** | **Valid Percent** |
|---|---|---|
| Very useful | 54 | 31. 8 |
| Useful and can help in minimizing the fraud losses | 52 | 30. 6 |
| Useful but not applicable | 50 | 29. 4 |
| Useless efforts | 14 | 8. 2 |
| **Total** | **170** | **100. 0** |

a. Just 8% from the respondents indicates that collaborative efforts between some destinations like (epaltel-banks) are useless efforts, and the rest of respondents agreed that it is useful effort.

b. The (FSA) findings strengthen the results above, the report said, there are encouraging signs of increased industry cooperation and strong support within firms for this nevertheless, more needs to be done in this area-not only to share raw data, but also to exchange information on the perpetrators of fraud.

c. Firms see this is critical to the success of anti-fraud measure. In particular there is strong support for various trade associations taking the lead and initiative, such as information sharing between firms coming out of this.

d. Firms believe there anti fraud efforts would benefit significantly from being able to obtain information relevant to frauds from government departments.

## Research Hypothesis:

**1- There is statistical relationship between the importance of fraud problem at Jawwal and the efficiency of fraud detection.**

**A. There is a statistical relationship between the importance of fraud problem within Jawwal and the number of fraud attacks which has been detected.**

***Table (50): Chi square test (The importance of anti fraud section * number of fraud cases which are discovered and detected)***

| Variable | Categories | Statistics | The number of fraud cases which are discovered and detected are | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Rare | Few and refer to the anti fraud efficiency | Moderate and refer to improving anti fraud | Numerous and refer to the need for more efficient anti fraud tools | |
| The importance of anti fraud section | Very important | Count | 13 | 51 | 77 | 5 | 146 |
| | | % of Total | 7. 6% | 30. 0% | 45. 3% | 2. 9% | 85. 9% |
| | Important | Count | 4 | 10 | 9 | 1 | 24 |
| | | % of Total | 2. 4% | 5. 9% | 5. 3% | . 6% | 14. 1% |
| | Total | Count | 17 | 61 | 86 | 6 | 170 |
| | | % of Total | 10. 0% | 35. 9% | 50. 6% | 3. 5% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 2. 481 | | | | | P –value = 0. 479 | | |

We used chi-square test to test if there is a relationship between the fraud importance and the number of fraud attacks which has been detected at significance level $\alpha \leq 0.05$, and the results shown in Table (50) which illustrate that the value of Pearson Chi-Square = 2.481 and the p-value = 0.479 which is greater than 0.05, so we fail to reject the null hypothesis m that means there is a no relationship between the fraud importance and the number of fraud attacks which has been detected at significance level $\alpha \leq 0.05$.

**B. There is statistical relationship between fraud importance and the kind of fraud attacks.**

*Table (51): Chi square test (The importance of fraud * the kind of fraud attacks)*

| variable | Categories | Statistics | The kind of fraud attacks | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | **A lot and imposes financial losses** | **Few but serious** | **Moderate** | **Neutral** | |
| The importance of anti fraud section | Very important | Count | 19 | 56 | 37 | 34 | 146 |
| | | % of Total | 11. 2% | 32. 9% | 21. 8% | 20. 0% | 85. 9% |
| | important | Count | 3 | 9 | 5 | 7 | 24 |
| | | % of Total | 1. 8% | 5. 3% | 2. 9% | 4. 1% | 14. 1% |
| | Total | Count | 22 | 65 | 42 | 41 | 170 |
| | | % of Total | 12. 9% | 38. 2% | 24. 7% | 24. 1% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 0. 473 | | | | | P –value = 0. 925 | | |

We used chi-square test to test if there is a relationship between the fraud importance and the kind of fraud attacks at significance level$\alpha \le 0.05$, and the results shown in Table (51) which illustrate that the value of Pearson Chi-Square = 2.4810 and the p-value = 0.479 which is greater than 0.05, so we fail to reject the null hypothesis m that means there is a no relationship between the fraud importance and the kind of fraud attacks at significance level $\alpha \le 0.05$.

**C. There is a statistical relationship between fraud importance and the effects of fraud**

***Table (52): Chi square test (The importance of fraud * the effects of fraud)***

| variable | Categories | Statistics | the effects of fraud | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Revenue and losses | Reputation | Service quality | All categories | |
| The importance of anti fraud section | Very important | Count | 20 | 10 | 1 | 115 | 146 |
| | | % of Total | 11. 8% | 5. 9% | . 6% | 67. 6% | 85. 9% |
| | important | Count | 4 | 3 | | 17 | 24 |
| | | % of Total | 2. 4% | 1. 8% | | 10. 0% | 14. 1% |
| | Total | Count | 24 | 13 | 1 | 132 | 170 |
| | | % of Total | 14. 1% | 7. 6% | . 6% | 77. 6% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 1. 321 | | | | | P –value = 0. 724 | | |

We used chi-square test to test if there is a relationship between the fraud importance and the effects of fraud at significance level $\alpha \leq 0.05$, and the results shown in Table (52) which illustrate that the value of Pearson Chi-Square= 1.321 and the p-value = 0.724 which is greater than 0.05, so we fail to reject the null hypothesis that means there is a no relationship between the fraud importance and the effects of fraud at significance level $\alpha \leq 0.05$.

**2. There is a statistical relationship between the anti fraud current tools, procedures and the efficiency of fraud detection.**

**A. There is a statistical relationship between number of fraud cases detected and the current criteria for identifying fraud**

***Table (53): Chi square test (The number of fraud cases which are discovered and detected * the current criteria to identify the fraudulent)***

| variable | Categories | Statistics | The current criteria to identify the fraudulent | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Efficient and leads to discover all of the fraud customers | Efficient but it's being relativity makes the fraud attacks possible | Needs to be more effective | Not efficient and there is need for a new criteria | |
| The number of fraud cases which are discovered and detected | Rare | Count | 6 | 6 | 4 | 1 | 17 |
| | | % of Total | 3. 5% | 3. 5% | 2. 4% | . 6% | 10. 0% |
| | Few and refer to the anti fraud efficiency | Count | 16 | 28 | 16 | 1 | 61 |
| | | % of Total | 9. 4% | 16. 5% | 9. 4% | . 6% | 35. 9% |
| | Moderate and refer to improving anti fraud | Count | 4 | 40 | 34 | 8 | 86 |
| | | % of Total | 2. 4% | 23. 5% | 20. 0% | 4. 7% | 50. 6% |
| | Numerous and refer to the need for more efficient anti fraud tools | Count | 1 | 2 | 3 | | 6 |
| | | % of Total | . 6% | 1. 2% | 1. 8% | | 3. 5% |
| | Total | Count | 27 | 76 | 57 | 10 | 170 |
| | | % of Total | 15. 9% | 44. 7% | 33. 5% | 5. 9% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 22. 387 | | | | | P –value = 0. 008 | | |

We used chi-square test to test if there is a relationship between The number of fraud cases which are discovered and detected and The current criteria to identify the fraudulent at significance level $\alpha \leq 0.05$, and the results shown in Table (53) which illustrate that the value of Pearson Chi-Square=22.387 and the p-value = 0.008 which is less than 0.05, so we reject the null hypothesis that means there is a relationship between the number of fraud cases which are discovered and detected and the current criteria to identify the fraudulent at significance level $\alpha \leq 0.05$.

**B. There is relationship between the fraud attacks and the current fraud detection tools**

***Table (54): Chi square test (The number of fraud cases which are discovered and detected * Current fraud detection tools)***

| **variable** | **Categories** | **Statistics** | **Current fraud detection tools** | | | | **Total** |
|---|---|---|---|---|---|---|---|
| | | | **Comprehensive and reliable** | **Reliable but not comprehensive** | **A need to more efficient tools there** | **one efficient tool will be more accurate** | |
| The number of fraud cases which are discovered and detected | Rare | Count | 6 | 7 | 3 | 1 | 17 |
| | | % of Total | 3. 5% | 4. 1% | 1. 8% | . 6% | 10. 0% |
| | Few and refer to the anti fraud efficiency | Count | 17 | 24 | 9 | 11 | 61 |
| | | % of Total | 10. 0% | 14. 1% | 5. 3% | 6. 5% | 35. 9% |
| | Moderate and refer to improving anti fraud | Count | 3 | 38 | 24 | 21 | 86 |
| | | % of Total | 1. 8% | 22. 4% | 14. 1% | 12. 4% | 50. 6% |
| | Numerous and refer to the need for more efficient anti fraud tools | Count | 1 | 3 | | 2 | 6 |
| | | % of Total | . 6% | 1. 8% | | 1. 2% | 3. 5% |
| | Total | Count | 27 | 72 | 36 | 35 | 170 |
| | | % of Total | 15. 9% | 42. 4% | 21. 2% | 20. 6% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 25. 622 | | | | | P –value = 0. 002 | | |

We used chi-square test to test if there is a relationship between The number of fraud cases which are discovered and detected and Current fraud detection tools at significance level $\alpha \le 0.05$, and the results shown in Table (54) which illustrate that the value of Pearson Chi-Square = 25.622 and the p-value = 0.002 which is less than 0.05, so we reject the null hypothesis that means there is a relationship between The number of fraud cases which are discovered and detected and Current fraud detection tools at significance level $\alpha \le 0.05$.

**C. There is a statistical relationship between current fraud detection tools and the anti fraud system program**

***Table (55): Chi square test (Current fraud detection tools * The fraud management system)***

| variable | Categories | Statistics | The current criteria to identify the fraudulent | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Comprehensive and reliable1 | Reliable but not comprehensive | Needs update and modification | Jawwal needs to employ new program | |
| Current fraud detection tools | Comprehensive and reliable | Count | 16 | 11 | 3 | 2 | 32 |
| | | % of Total | 9. 4% | 6. 5% | 1. 8% | 1. 2% | 18. 8% |
| | Reliable but not comprehensive | Count | 7 | 25 | 15 | 8 | 55 |
| | | % of Total | 4. 1% | 14. 7% | 8. 8% | 4. 7% | 32. 4% |
| | A need to more efficient tools there | Count | 3 | 29 | 14 | 19 | 65 |
| | | % of Total | 1. 8% | 17. 1% | 8. 2% | 11. 2% | 38. 2% |
| | one efficient tool will be more accurate | Count | 1 | 7 | 4 | 6 | 18 |
| | | % of Total | . 6% | 4. 1% | 2. 4% | 3. 5% | 10. 6% |
| | Total | Count | 27 | 72 | 36 | 35 | 170 |
| | | % of Total | 15. 9% | 42. 4% | 21. 2% | 20. 6% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 41. 969 | | | | | | P –value = 0. 000 | |

We used chi-square test to test if there is a relationship between Current fraud detection tools and The fraud management system at significance level $\alpha \leq 0.05$, and the results shown in Table (55) which illustrate that the value of Pearson Chi-Square = 41.969 and the p-value = 0.000 which is less than 0.05, so we reject the null hypothesis that so we reject the null hypothesis that means there is a relationship between Current fraud detection tools and The fraud management system at significance level $\alpha \leq 0.05$.

**D. There is statistical relationship between current fraud detection tools and billing**

***Table (56): Chi square test (Current fraud detection tools * billing reports)***

| variable | Categories | Statistics | billing reports | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Main tool to fraud detection | Supportive tool to fraud detection | . Supportive but not useful | Not reliable tool to depend on to detect fraud | |
| Current fraud detection tools | Comprehensive and reliable | Count | 12 | 12 | 3 | 3 | 30 |
| | | % of Total | 7. 1% | 7. 1% | 1. 8% | 1. 8% | 17. 6% |
| | Reliable but not comprehensive | Count | 10 | 36 | 17 | 17 | 80 |
| | | % of Total | 5. 9% | 21. 2% | 10. 0% | 10. 0% | 47. 1% |
| | A need to more efficient tools there | Count | 4 | 20 | 12 | 12 | 48 |
| | | % of Total | 2. 4% | 11. 8% | 7. 1% | 7. 1% | 28. 2% |
| | one efficient tool will be more accurate | Count | 1 | 4 | 4 | 3 | 12 |
| | | % of Total | . 6% | 2. 4% | 2. 4% | 1. 8% | 7. 1% |
| | **Total** | Count | 27 | 72 | 36 | 35 | 170 |
| | | % of Total | 15. 9% | 42. 4% | 21. 2% | 20. 6% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square =19. 279 | | | | | P –value = 0. 023 | | |

We used chi-square test to test if there is a relationship between current fraud detection tools and billing reports at significance level $\alpha \le 0.05$, and the results shown in Table (56) which illustrate that the value of Pearson Chi-Square= 19.279 and the p-value = 0.023 which is less than 0. 05, so we reject the null hypothesis that means there is a relationship between current fraud detection tools and billing reports at significance level $\alpha \le 0.05$

**E. There is statistical relationship between current fraud detection method and the black list window**

***Table (57): Chi square test (Current fraud detection tools * the black list window)***

| variable | Categories | Statistics | The black list window | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Comprehensive data base to discover the black listed customers | Comprehensive data base but not sufficient to discover all the black listed customers | Needs modification | Not efficient toll to discover the black listed customers | |
| Current fraud detection tools | Comprehensive and reliable | Count | 16 | 22 | 6 | 5 | 49 |
| | | % of Total | 9. 4% | 12. 9% | 3. 5% | 2. 9% | 28. 8% |
| | Reliable but not comprehensive | Count | 4 | 25 | 11 | 11 | 51 |
| | | % of Total | 2. 4% | 14. 7% | 6. 5% | 6. 5% | 30. 0% |
| | A need to more efficient tools there | Count | 7 | 23 | 18 | 19 | 67 |
| | | % of Total | 4. 1% | 13. 5% | 10. 6% | 11. 2% | 39. 4% |
| | one efficient tool will be more accurate | Count | | 2 | 1 | | 3 |
| | | % of Total | | 1. 2% | . 6% | | 1. 8% |
| | Total | Count | 27 | 72 | 36 | 35 | 170 |
| | | % of Total | 15. 9% | 42. 4% | 21. 2% | 20. 6% | 100. 0% |
| Pearson Chi-Square = 22. 778 | | | | | P –value = 0. 007 | | |

We used chi-square test to test if there is a relationship between current fraud detection tools and The black list window at significance level$\alpha \le 0.05$, and the results shown in Table (57) which illustrate that the value of Pearson Chi-Square=22.778 and the p-value=0.007 which is less than 0.05, so we reject the null hypothesis that means there is a relationship between current fraud detection tools and The black list window at significance level$\alpha \le 0.05$.

**3.There is a statistical relationship between sales target and the number of fraud attacks.**

**A. There is statistical relationship between the fraud attacks and sales target**

***Table (58): Chi square test (The fraud attacks * sales target)***

| variable | Categories | Statistics | sales target | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | **Sales person concentration on acquiring the target not the serve quality** | **Working under pressure** | **Carelessness to stop some of inaccurate superscription** | **All categories** | |
| the fraud attacks | A lot and imposes financial losses | Count | 5 | 3 | 2 | 12 | 22 |
| | | % of Total | 2. 9% | 1. 8% | 1. 2% | 7. 1% | 12. 9% |
| | Few but serious | Count | 11 | 15 | 4 | 35 | 65 |
| | | % of Total | 6. 5% | 8. 8% | 2. 4% | 20. 6% | 38. 2% |
| | Moderate | Count | 13 | 8 | 3 | 18 | 42 |
| | | % of Total | 7. 6% | 4. 7% | 1. 8% | 10. 6% | 24. 7% |
| | Neutral | Count | 14 | 5 | 3 | 19 | 41 |
| | | % of Total | 8. 2% | 2. 9% | 1. 8% | 11. 2% | 24. 1% |
| | Total | Count | 43 | 31 | 12 | 84 | 170 |
| | | % of Total | 25. 3% | 18. 2% | 7. 1% | 49. 4% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 6. 613 | | | | | P –value = 0. 677 | | |

We used chi-square test to test if there is a relationship between the fraud attacks and sales target at significance level$\alpha \le 0.05$, and the results shown in Table (58) which illustrate that the value of Pearson Chi-Square= 6.613 and the p-value = 0.677 which is greater than 0.05, so we fail to reject the null hypothesis that means there is no relationship between the fraud attacks and sales target at significance level$\alpha \le 0.05$.

**B. There is a statistical relationship between fraud attacks and sales personal**

***Table (59): Chi square test (The fraud attacks * The sales personnel)***

| variable | Categories | Statistics | The sales personnel | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Qualified and having sufficient knowledge of fraud problem | Qualified but the priority is for sales target only | Not qualified | flexible with fraud cases in negative way | |
| the fraud attacks | A lot and imposes financial losses | Count | 8 | 6 | 5 | 3 | 22 |
| | | % of Total | 4. 7% | 3. 5% | 2. 9% | 1. 8% | 12. 9% |
| | Few but serious | Count | 14 | 21 | 24 | 6 | 65 |
| | | % of Total | 8. 2% | 12. 4% | 14. 1% | 3. 5% | 38. 2% |
| | Moderate | Count | 18 | 15 | 9 | | 42 |
| | | % of Total | 10. 6% | 8. 8% | 5. 3% | | 24. 7% |
| | Neutral | Count | 18 | 13 | 9 | 1 | 41 |
| | | % of Total | 10. 6% | 7. 6% | 5. 3% | . 6% | 24. 1% |
| | Total | Count | 58 | 55 | 47 | 10 | 170 |
| | | % of Total | 34. 1% | 32. 4% | 27. 6% | 5. 9% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 15. 534 | | | | | P –value = 0. 077 | | |

We used chi-square test to test if there is a relationship between the fraud attacks and The sales personnel at significance level$\alpha \le 0.05$, and the results shown in Table (59) which illustrate that the value of Pearson Chi-Square=15.534 and the p-value = 0.077 which is greater than 0.05, so we fail to reject the null hypothesis that means there is no relationship between the fraud attacks and the sales personnel at significance level $\alpha \le 0.05$.

### C. There is a statistical relationship between fraud attacks and other resource of information regarding fraud cases

***Table (60): Chi square test (The fraud attacks * other resource of information regarding fraud cases)***

| variable | Categories | Statistics | other resource of information regarding fraud cases | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | efficient source to discover the fraud cases | efficient source and it is roll needs to more active | subordinate roll | inefficient roll | |
| the fraud attacks | A lot and imposes financial losses | Count | 9 | 3 | 10 | | 22 |
| | | % of Total | 5. 3% | 1. 8% | 5. 9% | | 12. 9% |
| | Few but serious | Count | 14 | 24 | 25 | 2 | 65 |
| | | % of Total | 8. 2% | 14. 1% | 14. 7% | 1. 2% | 38. 2% |
| | Moderate | Count | 16 | 12 | 11 | 3 | 42 |
| | | % of Total | 9. 4% | 7. 1% | 6. 5% | 1. 8% | 24. 7% |
| | Neutral | Count | 17 | 13 | 11 | | 41 |
| | | % of Total | 10. 0% | 7. 6% | 6. 5% | | 24. 1% |
| | Total | Count | 56 | 52 | 57 | 5 | 170 |
| | | % of Total | 32. 9% | 30. 6% | 33. 5% | 2. 9% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 14. 231 | | | | | P –value = 0. 114 | | |

We used chi-square test to test if there is a relationship between the fraud attacks and other resource of information regarding fraud cases at significance level $\alpha \le 0.05$, and the results shown in Table (60) which illustrate that the value of Pearson Chi-Square =14.231 and the p-value = 0.144 which is greater than 0.05, so we fail to reject the null hypothesis that means there is no relationship between the fraud attacks and other resource of information regarding fraud cases at significance level $\alpha \le 0.05$.

**4. There is a statistical relationship between programs, procedures, offers and fraud attacks.**

**A. There is statistical relationship between fraud attacks and the policies and procedures**

***Table (61): Chi square test (The fraud attacks * The policies and procedures)***

| variable | Categories | Statistics | The policies and procedures | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Clear about fraud problem | Unclear and there gabs | Unclear and incomprehensive | Unclear and need to be modified | |
| the fraud attacks | A lot and imposes financial losses | Count | 4 | 12 | 5 | 1 | 22 |
| | | % of Total | 2. 4% | 7. 1% | 2. 9% | . 6% | 12. 9% |
| | Few but serious | Count | 10 | 38 | 13 | 4 | 65 |
| | | % of Total | 5. 9% | 22. 4% | 7. 6% | 2. 4% | 38. 2% |
| | Moderate | Count | 13 | 21 | 5 | 3 | 42 |
| | | % of Total | 7. 6% | 12. 4% | 2. 9% | 1. 8% | 24. 7% |
| | Neutral | Count | 20 | 10 | 8 | 3 | 41 |
| | | % of Total | 11. 8% | 5. 9% | 4. 7% | 1. 8% | 24. 1% |
| | Total | Count | 47 | 81 | 31 | 11 | 170 |
| | | % of Total | 27. 6% | 47. 6% | 18. 2% | 6. 5% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 19. 081 | | | | | P –value = 0. 025 | | |

We used chi-square test to test if there is a relationship between the fraud attacks and The policies and procedures at significance level $\alpha \le 0.05$, and the results shown in Table (61) which illustrate that the value of Pearson Chi-Square= 19.081 and the p-value = 0.025 which is less than 0.05, so we reject the null hypothesis that means there is a relationship between the fraud attacks and The policies and procedures at significance level $\alpha \le 0.05$.

**B. There is statistical relationship between fraud attacks and promotions and offers**

***Table (62): Chi square test (The fraud attacks * promotions and offers)***

| variable | Categories | Statistics | promotions and offers | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | **Comprehensive and accurate** | **Skillful but contains gaps to defraud company** | **not accurate and there is gaps to defraud ate the company** | **They are not consider window to defraud ate** | |
| the fraud attacks | A lot and imposes financial losses | Count | 3 | 11 | 8 | | 22 |
| | | % of Total | 1. 8% | 6. 5% | 4. 7% | | 12. 9% |
| | Few but serious | Count | 8 | 28 | 16 | 13 | 65 |
| | | % of Total | 4. 7% | 16. 5% | 9. 4% | 7. 6% | 38. 2% |
| | Moderate | Count | 8 | 23 | 5 | 6 | 42 |
| | | % of Total | 4. 7% | 13. 5% | 2. 9% | 3. 5% | 24. 7% |
| | Neutral | Count | 11 | 14 | 6 | 10 | 41 |
| | | % of Total | 6. 5% | 8. 2% | 3. 5% | 5. 9% | 24. 1% |
| | Total | Count | 30 | 76 | 35 | 29 | 170 |
| | | % of Total | 17. 6% | 44. 7% | 20. 6% | 17. 1% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 16. 389 | | | | | P –value = 0. 059 | | |

We used chi-square test to test if there is a relationship between the fraud attacks and promotions and offers at significance level $\alpha \le 0.05$, and the results shown in Table (62) which illustrate that the value of Pearson Chi-Square=16.389 and the p-value = 0.059 which is greater than 0.05, so we fail to reject the null hypothesis that means there is no relationship between the fraud attacks and promotions and offers at significance level $\alpha \le 0.05$.

## C. There is a statistical relationship between fraud attacks and guarantee policy

***Table (63): Chi square test (The fraud attacks * The guarantee policy)***

| variable | Categories | Statistics | The guarantee policy | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Suitable | Good recovery in case the customer became fraudulent | Suitable but need to be modified | unsuitable for the whole customers | |
| the fraud attacks | A lot and imposes financial losses | Count | 3 | 4 | 9 | 6 | 22 |
| | | % of Total | 1. 8% | 2. 4% | 5. 3% | 3. 5% | 12. 9% |
| | Few but serious | Count | 13 | 16 | 19 | 17 | 65 |
| | | % of Total | 7. 6% | 9. 4% | 11. 2% | 10. 0% | 38. 2% |
| | Moderate | Count | 12 | 11 | 10 | 9 | 42 |
| | | % of Total | 7. 1% | 6. 5% | 5. 9% | 5. 3% | 24. 7% |
| | Neutral | Count | 13 | 7 | 15 | 6 | 41 |
| | | % of Total | 7. 6% | 4. 1% | 8. 8% | 3. 5% | 24. 1% |
| | Total | Count | 41 | 38 | 53 | 38 | 170 |
| | | % of Total | 24. 1% | 22. 4% | 31. 2% | 22. 4% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 7. 522 | | | | | P –value = 0. 587 | | |

We used chi-square test to test if there is a relationship between the fraud attacks and The guarantee policy at significance level $\alpha \le 0.05$, and the results shown in Table (63) which illustrate that the value of Pearson Chi-Square= 7.522 and the p-value = 0.587 which is greater than 0.05, so we fail to reject the null hypothesis that means there is no relationship between the fraud attacks and the guarantee policy significance level $\alpha \le 0.05$

**D. There is statistical relationship between fraud attacks and the accelerate modifying of policies and procedures**

*Table (64): Chi square test (The fraud attacks * The accelerate modifying of policies and procedures)*

| variable | Categories | Statistics | The accelerate modifying of policies and procedures | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Useful and serve work | Useful but need to be more slow | Useful but separate the employee attention | Unuseful and not serve the work | |
| the fraud attacks | A lot and imposes financial losses | Count | 7 | 5 | 8 | 2 | 22 |
| | | % of Total | 4. 1% | 2. 9% | 4. 7% | 1. 2% | 12. 9% |
| | Few but serious | Count | 16 | 19 | 28 | 2 | 65 |
| | | % of Total | 9. 4% | 11. 2% | 16. 5% | 1. 2% | 38. 2% |
| | Moderate | Count | 7 | 19 | 13 | 3 | 42 |
| | | % of Total | 4. 1% | 11. 2% | 7. 6% | 1. 8% | 24. 7% |
| | Neutral | Count | 11 | 9 | 17 | 4 | 41 |
| | | % of Total | 6. 5% | 5. 3% | 10. 0% | 2. 4% | 24. 1% |
| | Total | Count | 41 | 52 | 66 | 11 | 170 |
| | | % of Total | 24. 1% | 30. 6% | 38. 8% | 6. 5% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 9. 254 | | | | | P –value = 0. 414 | | |

We used chi-square test to test if there is a relationship between the fraud attacks and The accelerate modifying of policies and procedures at significance level $\alpha \le 0.05$, and the results shown in Table (64) which illustrate that the value of Pearson Chi-Square =9.254 and the p-value = 0.141 which is greater than 0. 05, so we fail to reject the null hypothesis that means there is no relationship between the fraud attacks and The accelerate modifying of policies and procedures significance level $\alpha \le 0.05$.

**E. There is statistical relationship between the steps of fraud detection and the new subscription and agreement documents**

***Table (65): Chi square test (The steps of fraud detection * the new subscription and agreement documents)***

| variable | Categories | Statistics | the new subscription and agreement documents | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Comprehensive | Not comprehensive | Not efficient | Needs to be more strict | |
| the steps of fraud detection | subscription | Count | 25 | 34 | 8 | 21 | 88 |
| | | % of Total | 14. 7% | 20. 0% | 4. 7% | 12. 4% | 51. 8% |
| | Activation | Count | 13 | 15 | 1 | 4 | 33 |
| | | % of Total | 7. 6% | 8. 8% | . 6% | 2. 4% | 19. 4% |
| | Fraud prevention | Count | 10 | 8 | 4 | 5 | 27 |
| | | % of Total | 5. 9% | 4. 7% | 2. 4% | 2. 9% | 15. 9% |
| | Fraud detection | Count | 5 | 11 | 1 | 5 | 22 |
| | | % of Total | 2. 9% | 6. 5% | . 6% | 2. 9% | 12. 9% |
| | Total | Count | 53 | 68 | 14 | 35 | 170 |
| | | % of Total | 31. 2% | 40. 0% | 8. 2% | 20. 6% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 7. 954 | | | | | P –value = 0. 539 | | |

We used chi-square test to test if there is a relationship between the steps of fraud detection and the new subscription and agreement documents at significance level $\alpha \leq 0.05$, and the results shown in Table (65) which illustrate that the value of Pearson Chi-Square =7.954 and the p-value = 0.539 which is greater than 0.05, so we fail to reject the null hypothesis that means there is no relationship between the steps of fraud detection and the new subscription and agreement documents at significance level $\alpha \leq 0.05$.

## 5. There is statistical relationship between employee's awareness and fraud attacks

## A. There is statistical relationship between fraud attacks and Jawwal employees

***Table (66): Chi square test (The fraud attacks * Jawwal employee)***

| variable | Categories | Statistics | Jawwal employee | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Qualified enough to deal with fraud problem and fraudulent | Qualified but needs training | Not qualified | No need for fraud prevention and detection qualifications for most employees | |
| the fraud attacks | A lot and imposes financial losses | Count | 6 | 9 | 6 | 1 | 22 |
| | | % of Total | 3. 5% | 5. 3% | 3. 5% | . 6% | 12. 9% |
| | Few but serious | Count | 9 | 26 | 25 | 5 | 65 |
| | | % of Total | 5. 3% | 15. 3% | 14. 7% | 2. 9% | 38. 2% |
| | Moderate | Count | 6 | 24 | 10 | 2 | 42 |
| | | % of Total | 3. 5% | 14. 1% | 5. 9% | 1. 2% | 24. 7% |
| | Neutral | Count | 11 | 18 | 10 | 2 | 41 |
| | | % of Total | 6. 5% | 10. 6% | 5. 9% | 1. 2% | 24. 1% |
| | Total | Count | 32 | 77 | 51 | 10 | 170 |
| | | % of Total | 18. 8% | 45. 3% | 30. 0% | 5. 9% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 8. 521 | | | | | P –value = 0. 483 | | |

We used chi-square test to test if there is a relationship between the fraud attacks and Jawwal employee at significance level $\alpha \leq 0.05$, and the results shown in Table (66) which illustrate that the value of Pearson Chi-Square= 8.521 and the p-value = 0.483 which is greater than 0.05, so we fail to reject the null hypothesis that means there is no relationship between the fraud attacks and Jawwal employee at significance level $\alpha \leq 0.05$.

**B. There is statistical relationship between fraud attacks and the definition of the fraudulent**

*Table (67): Chi square test (The fraud attacks * the fraudulent customer)*

| variable | Categories | Statistics | The fraudulent customer | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Had the intention to defraud ate | Had Bad experience with the company | Utilize the system gaps | All categories | |
| the fraud attacks | A lot and imposes financial losses | Count | 8 | 3 | 2 | 9 | 22 |
| | | % of Total | 4. 7% | 1. 8% | 1. 2% | 5. 3% | 12. 9% |
| | Few but serious | Count | 13 | | 9 | 43 | 65 |
| | | % of Total | 7. 6% | | 5. 3% | 25. 3% | 38. 2% |
| | Moderate | Count | 9 | 3 | 11 | 19 | 42 |
| | | % of Total | 5. 3% | 1. 8% | 6. 5% | 11. 2% | 24. 7% |
| | Neutral | Count | 10 | 1 | 8 | 22 | 41 |
| | | % of Total | 5. 9% | . 6% | 4. 7% | 12. 9% | 24. 1% |
| | Total | Count | 40 | 7 | 30 | 93 | 170 |
| | | % of Total | 23. 5% | 4. 1% | 17. 6% | 54. 7% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 16. 989 | | | | | P –value = 0. 049 | | |

We used chi-square test to test if there is a relationship between the fraud attacks and The fraudulent customer at significance level $\alpha \leq 0.05$, and the results shown in Table (67) which illustrate that the value of Pearson Chi-Square= 16.989 and the p-value=0.049 which is less than 0.05, so we reject the null hypothesis that means there is a relationship between the fraud attacks and The fraudulent customer at significance level $\alpha \leq 0.05$.

**C. There is statistical relationship between fraud attacks and criteria of defining the fraudulent**

***Table (68): Chi square test (The fraud attacks * criteria of defending the fraudulent)***

| variable | Categories | Statistics | criteria if defending the fraudulent | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | The sudden change in his usage (calls /services) | The kind of service the customer requests | The number of lines requested | All categories | |
| the fraud attacks | A lot and imposes financial losses | Count | 2 | 4 | 4 | 12 | 22 |
| | | % of Total | 1. 2% | 2. 4% | 2. 4% | 7. 1% | 12. 9% |
| | Few but serious | Count | 8 | 6 | 2 | 49 | 65 |
| | | % of Total | 4. 7% | 3. 5% | 1. 2% | 28. 8% | 38. 2% |
| | Moderate | Count | 6 | 4 | 3 | 29 | 42 |
| | | % of Total | 3. 5% | 2. 4% | 1. 8% | 17. 1% | 24. 7% |
| | Neutral | Count | 1 | 1 | 4 | 35 | 41 |
| | | % of Total | . 6% | . 6% | 2. 4% | 20. 6% | 24. 1% |
| | Total | Count | 17 | 15 | 13 | 125 | 170 |
| | | % of Total | 10. 0% | 8. 8% | 7. 6% | 73. 5% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 14. 818 | | | | | P –value = 0. 096 | | |

We used chi-square test to test if there is a relationship between the fraud attacks and criteria if defending the fraudulent at significance level $\alpha \le 0.05$, and the results shown in Table (68) which illustrate that the value of Pearson Chi-Square=14.818 and the p-value=0.096 which is greater than 0.05, so we fail to reject the null hypothesis that means there is no relationship between the fraud attacks and criteria if defending the fraudulent at significance level $\alpha \le 0.05$.

**6. There is statistical relationship between values added services and number of fraud attacks**

**A. There is statistical relationship between fraud attacks and the most services vulnerable to fraud**

***Table (69): Chi square test (The fraud attacks * the most service consider vulnerable to the fraud attacks)***

| variable | Categories | Statistics | The most service consider vulnerable to the fraud attacks | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | International roaming | International | Sort massage service | Wape and interne | |
| the fraud attacks | A lot and imposes financial losses | Count | 10 | 8 | 3 | 1 | 22 |
| | | % of Total | 5. 9% | 4. 7% | 1. 8% | . 6% | 12. 9% |
| | Few but serious | Count | 31 | 23 | 4 | 7 | 65 |
| | | % of Total | 18. 2% | 13. 5% | 2. 4% | 4. 1% | 38. 2% |
| | Moderate | Count | 17 | 12 | 7 | 6 | 42 |
| | | % of Total | 10. 0% | 7. 1% | 4. 1% | 3. 5% | 24. 7% |
| | Neutral | Count | 15 | 14 | 4 | 8 | 41 |
| | | % of Total | 8. 8% | 8. 2% | 2. 4% | 4. 7% | 24. 1% |
| | Total | Count | 73 | 57 | 18 | 22 | 170 |
| | | % of Total | 42. 9% | 33. 5% | 10. 6% | 12. 9% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 7. 006 | | | | | P –value = 0. 637 | | |

We used chi-square test to test if there is a relationship between the fraud attacks and The most service consider vulnerable to the fraud attacks at significance level $\alpha \le 0.05$, and the results shown in Table (69) which illustrate that the value of Pearson Chi-Square=7.006 and the p-value = 0.637 which is greater than 0.05, so we fail to reject the null hypothesis that means there is no relationship between the fraud attacks and The most service consider vulnerable to the fraud attacks significance level $\alpha \le 0.05$.

### B. There is statistical relationship between fraud attacks and corporate department

***Table (70): Chi square test (The fraud attacks * corporate department)***

| variable | Categories | Statistics | corporate department | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | **Corporate sales policy and the absent if guarantee in most of activated lines** | **Sales target** | **Activating some services such as ID and IR without guarantee** | **All categories** | |
| the fraud attacks | A lot and imposes financial losses | Count | 6 | 3 | 3 | 10 | 22 |
| | | % of Total | 3. 5% | 1. 8% | 1. 8% | 5. 9% | 12. 9% |
| | Few but serious | Count | 10 | 18 | 3 | 34 | 65 |
| | | % of Total | 5. 9% | 10. 6% | 1. 8% | 20. 0% | 38. 2% |
| | Moderate | Count | 7 | 5 | 2 | 28 | 42 |
| | | % of Total | 4. 1% | 2. 9% | 1. 2% | 16. 5% | 24. 7% |
| | Neutral | Count | 6 | 9 | 5 | 21 | 41 |
| | | % of Total | 3. 5% | 5. 3% | 2. 9% | 12. 4% | 24. 1% |
| | Total | Count | 29 | 35 | 13 | 93 | 170 |
| | | % of Total | 17. 1% | 20. 6% | 7. 6% | 54. 7% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 10. 263 | | | | | P –value = 0. 330 | | |

We used chi-square test to test if there is a relationship between the fraud attacks and The corporate department at significance level $\alpha \leq 0.05$, and the results shown in Table (70) which illustrate that the value of Pearson Chi-Square = 10.263and the p-value = 0.330 which is greater than 0.05, so we fail to reject the null hypothesis that means there is no relationship between the fraud attacks and corporate department at significance level $\alpha \leq 0.05$.

**C. There is statistical relationship between the fraud attacks and the services activated by default**

*Table (71): Chi square test (The fraud attacks * the services activated)*

| variable | Categories | Statistics | The services activated | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Increasing company vulnerability to fraud | Useful and serving customer | Need to be more strict | It is not related to fraud attacks | |
| the fraud attacks | A lot and imposes financial losses | Count | 5 | 4 | 8 | 5 | 22 |
| | | % of Total | 2. 9% | 2. 4% | 4. 7% | 2. 9% | 12. 9% |
| | Few but serious | Count | 9 | 13 | 24 | 19 | 65 |
| | | % of Total | 5. 3% | 7. 6% | 14. 1% | 11. 2% | 38. 2% |
| | Moderate | Count | 6 | 11 | 12 | 13 | 42 |
| | | % of Total | 3. 5% | 6. 5% | 7. 1% | 7. 6% | 24. 7% |
| | Neutral | Count | 5 | 6 | 6 | 24 | 41 |
| | | % of Total | 2. 9% | 3. 5% | 3. 5% | 14. 1% | 24. 1% |
| | Total | Count | 25 | 34 | 50 | 61 | 170 |
| | | % of Total | 14. 7% | 20. 0% | 29. 4% | 35. 9% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 15. 281 | | | | | P –value = 0. 083 | | |

We used chi-square test to test if there is a relationship between the fraud attacks and The services activated at significance level $\alpha \leq 0.05$, and the results shown in Table (71) which illustrate that the value of Pearson Chi-Square = 15.281 and the p-value = 0.083 which is greater than 0.05, so we fail to reject the null hypothesis that means there is no relationship between the fraud attacks and The services activated at significance level $\alpha \leq 0.05$.

**7. There is a statistical relationship between pricing policy and fraud attacks**

**A. There is statistical relationship between fraud attacks and pricing policy**

***Table (72): Chi square test (The fraud attacks * The pricing policy)***

| **variable** | **Categories** | **Statistics** | **The pricing policy** | | | | **Total** |
|---|---|---|---|---|---|---|---|
| | | | **Suitable and not consider motive to defraud ate the company** | **High** | **Moderate** | **Unsuitable and consider motive to defraud ate the company** | |
| the fraud attacks | A lot and imposes financial losses | Count | 9 | 4 | 7 | 2 | 22 |
| | | % of Total | 5. 3% | 2. 4% | 4. 1% | 1. 2% | 12. 9% |
| | Few but serious | Count | 23 | 5 | 30 | 7 | 65 |
| | | % of Total | 13. 5% | 2. 9% | 17. 6% | 4. 1% | 38. 2% |
| | Moderate | Count | 13 | 7 | 20 | 2 | 42 |
| | | % of Total | 7. 6% | 4. 1% | 11. 8% | 1. 2% | 24. 7% |
| | Neutral | Count | 20 | 5 | 14 | 2 | 41 |
| | | % of Total | 11. 8% | 2. 9% | 8. 2% | 1. 2% | 24. 1% |
| | Total | Count | 65 | 21 | 71 | 13 | 170 |
| | | % of Total | 38. 2% | 12. 4% | 41. 8% | 7. 6% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 7. 828 | | | | | | P –value = 0. 552 | |

We used chi-square test to test if there is a relationship between the fraud attacks and The pricing policy at significance level $\alpha \leq 0.05$, and the results shown in Table (72) which illustrate that the value of Pearson Chi-Square = 0.7828 and the p-value = 0.552 which is greater than 0.05, so we fail to reject the null hypothesis that means there is no relationship between the fraud attacks and the pricing policy at significance level $\alpha \leq 0.05$.

**B. There is a statistical relationship between fraud attacks and the insolvent customer**

***Table (73): Chi square test (The fraud attacks * the insolvent customer)***

| variable | Categories | Statistics | the insolvent customer | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Intention to not defraud ate | Commitment | Possibility to pay the due amounts | All categories | |
| the fraud attacks | A lot and imposes financial losses | Count | 7 | 1 | 4 | 10 | 22 |
| | | % of Total | 4. 1% | . 6% | 2. 4% | 5. 9% | 12. 9% |
| | Few but serious | Count | 10 | 4 | 4 | 47 | 65 |
| | | % of Total | 5. 9% | 2. 4% | 2. 4% | 27. 6% | 38. 2% |
| | Moderate | Count | 8 | | 3 | 31 | 42 |
| | | % of Total | 4. 7% | | 1. 8% | 18. 2% | 24. 7% |
| | Neutral | Count | 9 | 3 | 4 | 25 | 41 |
| | | % of Total | 5. 3% | 1. 8% | 2. 4% | 14. 7% | 24. 1% |
| | Total | Count | 34 | 8 | 15 | 113 | 170 |
| | | % of Total | 20. 0% | 4. 7% | 8. 8% | 66. 5% | 100. 0% |
| | | | | | | | |
| Pearson Chi-Square = 10. 392 | | | | | | P –value = 0. 320 | |

We used chi-square test to test if there is a relationship between the fraud attacks and the insolvent customer at significance level $\alpha \leq 0.05$, and the results shown in Table (73) which illustrate that the value of Pearson Chi-Square = 10.392 and the p-value = 0.320 which is greater than 0.05, so we fail to reject the null hypothesis that means there is no relationship between the fraud attacks and the insolvent customer at significance level $\alpha \leq 0.05$.

*Table (74): Summary of Hypothesis*

| Main hypothesis | Sup hypothesis | Result |
|---|---|---|
| 1. There is statistical relationship between the importance of fraud problem within Jawwal and the efficiency of fraud detection | There is a statistical relationship between the importance of fraud problem within Jawwal and the number of fraud attacks which has been detected | Rejected |
| | There is statistical relationship between fraud importance and the kind of fraud attacks | Rejected |
| | There is a statistical relationship between fraud importance and the effects of fraud | Rejected |
| 2. There is a statistical relationship between the anti fraud current tools, procedures and the efficiency of fraud detection | There is a statistical relationship between number of fraud cases detected and the current criteria for identifying fraud | Accepted |
| | there is relationship between the fraud attacks and the current fraud detection tools | Accepted |
| | There is a statistical relationship between current fraud detection tools and the anti fraud system program | Accepted |
| | There is statistical relationship between current fraud detection tools and billing | Accepted |
| | There is statistical relationship between current fraud detection method and the black list window | Accepted |
| 3. There is a statistical relationship between sales target and the number of fraud attacks. | There is a statistical relationship between the fraud attacks and sales target | Rejected |
| | there is a statistical relationship between fraud attacks and sales person | Rejected |
| | There is a statistical relationship between fraud attacks and other resource of information regarding fraud cases | Rejected |
| 4. There is a statistical relationship between programs, procedures, offers and fraud attacks. | there is statistical relationship between fraud attacks and the policies and procedures | Accepted |
| | There is relationship between fraud attacks and promotions and offers | Rejected |
| | there is a statistical relationship between fraud attacks and guarantee policy | Rejected |
| | There is relationship between fraud attacks and the accelerate modifying of policies and procedures | Rejected |
| | there is relationship between the steps of fraud detection and the new subscription and agreement documents | Rejected |

| Main hypothesis | Sup hypothesis | Result |
|---|---|---|
| 5. There is a statistical relationship between employees awareness and fraud attacks | There is relationship between fraud attacks and Jawwal employees | Rejected |
| | There is a statistical relationship between fraud attacks and the definition of the fraudulent | Accepted |
| | There is a statistical relationship between fraud attacks and criteria of defining the fraudulent | Rejected |
| 6. There is a statistical relationship between value added services and number of fraud attacks | There is a statistic relationship between fraud attacks and the most services vulnerable to fraud | Rejected |
| | There is no relationship between fraud attacks and increasing number of fraud cases in corporate department | Rejected |
| | There is statistical relationship between the fraud detection steps and the services activated by default | Rejected |
| 7. There is a statistical relationship between pricing policy and fraud attacks | There is relationship between fraud attacks and pricing policy | Rejected |
| | There is a statistical relationship between fraud attacks and the insolvent customer | Rejected |

# CHAPTER [7]

# CONCLUSION AND RECOMMENDATION

**This chapter presents the major conclusion and recommendations about the thesis**

## Conclusion:

The research provides detail analysis of fraud problem that Jawwal Company may be encountered with. Also a systematic directions s is given to avoid and deal with such a problem, though the following points are extremely important.

1. Jawwal did not have fraud strategy or clear mandate on what will be covered by the fraud team that means inability to determine the fraud risk or level of exposure.
2. Lack of or ill defined fraud policies and practices, that means failing to produce and work to standard operating procedures.
3. Jawwal in it is way to fight fraud is more reactive than proactive.
4. Limited use of the available technology, FMS deployed but failing to maxims its capabilities.
5. Fraud Teams unable to terminate fraud -Internal politics and conflicts of interest.
6. Unclear mission statements, Fraud Teams spending weeks including doing field investigations, building many of pages of prosecution material, for a single case of subscription Fraud , this is totally ineffective use of resources.
7. Limited and untrained resources for the employees.

## Recommendation:

1. As for Jawwal, the basic principles for good fraud management are to ensure that detection and prevention of fraud requires an understanding of the actual threat, that means know what is the fraud incident, What is the motive for committing the fraud, what is the periods for the fraud attacks, time farm, Persons involved, is it externally or internally, and finally the ways it is perpetrated, the approach, method used.
2. Jawwal company, it must not get targeted by becoming a soft touch for fraud" the easy option, the unguarded victim".

3. The company needs to learn from the mistakes of others, and learn how to be adapted and initiative in it is approach.

4. It is better for Jawwal to target its' vulnerable business areas before the fraudster target it.

5. The company must acquire, highly professional FMS .

6. Fraud detection current tolls must be modified.

7. There is a must to have, sufficient policies and procedures related to the fraud problem in place

8. Jawwal Company need to think whether they have sufficient expertise and knowledge to deal with fraud.

9. Jawwal need to think whether they have sufficient management support in fraud management aspect.

10. Jawwal needs to e open minded to the internal risk

11. Jawwal needs to be e aware of how fraud department e perceived by the employees, necessary evil or an essential part of the company?

12. Fraud team should think like a fraudster when assessing the risk.

13. Finally the researcher hopes that the results of this research not only can benefit Jawwal company (case study), but also can be extended to other similar companies in the region.

# References

- "Apri. [September 2004], if it sounds too good to be true-local prosecutors 'experience of fightingtelecommunicationfraud,available:http://www.nadaa-apri.org/pdf/sounds-tpp-good.pdf,[accessed on 26 October 2009]".

- A P .Agrawal ,"telecom fraud management 2010,KPMG ,available: http://www.cerebralbusiness.com/telecom/presentations/Arpita%20Pal%20Agrawal.pdf, [accessed on1December 2010]",2010

- A. Bavosa," GPRS Security threats and solution recommendations, Juniper network, white paper, available: http://s-tools1.juniper.net/solutions/literature/white_papers/200074 ,[accessed on13 May 2010]".2004

- A. Graycar ,R.Smith," Australian institute of Criminology ,Identifying and Responding to Electronic fraud Risk," proceeding, of the ,30th Australian Registers conferenceCanbera,available:http://www.popcenter.org/problems/credit_card_fraud/PDFs/Graycar%26Smith.pdf,[accessed on 25 march2010]",2002

- A.Banjoko ,"using the circle of trust to enhance fraud management in developing markets, GRAPA, available: www.telecom-fraud.org ,[accessed on16 June 2010]",2009

- A.Krenker,M.Volk,U.Sedlar,J. Bester and A.Kos ,"Bidirectional Artificial Neural Network For Mobile Phone Fraud Detection .available: http://www.ltfe.org/wp-content/uploads/2009/07/AKrenker2009-Bidirectional-artificial-neural-networks.pdf ,[ accessed on 20September 2010]",2009

- ACFE association of certified fraud examiners,"ACFE the report to the nation on the occupational fraud and abuse, technical report,"2006.

- AFP association for financial prepositional," payment fraud survey, report of survey result, ,underwritten by electronic paymentsnetwork,Available:http://www.afponline.org/pub/pdf/2007PaymentsFraudSurvey.pdf, [accessed on13 October 2010]",2007

- Anonymous " who commit fraud and why :chapter 2 .p 18.available: http://www.swlearning.com/pdfs/chapter/053872689X_2.PDF , [ accessed October 2010]",2003

- Arab advisor group ,strategic research service ,"Palestine's line grow by 18.9% In H12010",2010

- AT&T,"Business subscription and equipment fraud prevention, available: http://www.atlantacellular.com/posdotcom/helpful%20admin%20forms/Business%20Subcription%20Fraud%20Job%20Aid.pdf [accessed on11 November 2010]", 2009

- B.schneier,"social engineering: people hacking, control essential. Enterprise risk management. available: http://69.89.31.151/~emrikcom/wp-content/uploads/2010/07/ERMNewsletter_november_2009.pdf, [accessed on15 May 2010]",2009

- B/OSS," Telecom fraud on raise, available: http://www.billingworld.com/articles/2004/07/telecom-fraud-on-the-rise.aspx, [accessed on25 June 2010]",2004

- B/OSS," Top telecom fraud and how to stop them, avilable:http://www.billingworld.com/articles/2007/01/top-telco-frauds-and-how-to-stop-them.aspx , [accessed on 15 October 2010]",2007

- BAKER TILLY," Anti –fraud management survey results, magnify your anti fraud management, available: http://www.bakertilly.com/cms/public/userfiles/40eb699b88a3fbd294f043905ecdb9b1e448003f/00d16e0290b6ce8f3262342142d8ed8f093ec767Anti-fraud%20management%20survey_2008.04.pdf ,[accessed on 29 march 2010]", 2008

- Bearing point, management & technology consultants, " fraud management trends in insurance, white paper, available: http://www.bearingpoint.ru/images/content/Fraud_Management_BearingPoint_Study.pdf ,[accessed on 13 May2010", 2008

- Business issue, "credit risk and bad debit "understanding receivables management problems and solutions for telecommunication ,media and entertainment sector available: http://www.scribd.com/doc/28155799/Credit-Risk-and-Bad-Debt-in-Telecommunications, [accessed on 25 March 2010]",2009

- C.brookson," smart card cloning is easy (GSM SIMs), available: http://www.brookson.com/gsm/cardclone.pdf , [accesses on19 June 2010]", 2005

- C.Brookson,c.farrel,j.mailley,s.whithead and d.zumele ,"TCT product proofing against the crime ,ETSI white paper no.5 ,available: http://www.etsi.org/WebSite/document/Technologies/ETSI-WP5_Product_Proofing.pdf ,[accessed on4 September 2009]",2007

- C.ebner," smart card production environment, available: www.sprenger.com ,[accessed on13 may 2010]".

- C.Yates ,"mobile phone issues-what risks associated with their use by our youth ,available: http://www.netsafe.org.nz/Doc_Library/netsafepapers_colinyates_mobile.pdf , [accessed on 27 march 2010]",2003.

- CCK -Communication commission of Kenya, Fact sheet "internet security and privacy", available: http://www.cck.go.ke/consumers/internet_services/downloads/internet_security_privacyfull.pdf ,[accessed 15 October 2010]", 2008

- Cellular phone news," Earth Vision Cellular prepaid service VS post paid services. Available: http://www.cellularphonenews.com/ebook/prepaid_e.html [accessed on 23 August 2010]".

- Cellular-news , available: http://www.cellular-news.com/story/16222.php, [accessed 21 march 2010]",2006

- Celtel group, "presentation of the public inquiry organized by the NCC toward a national scheme to curtail the theft of Mobil phone, available: http://www.ncc.gov.ng/cab/Curtail%20Theft/Prestn%20(VNL-NCC)%20Consultn%20on%20Curbing%20Mobile%20Phone%20Theft%20rev1.pdf ,accessed on 13 may 2010]". 2006

- CFCA, "Communication fraud control association results of worldwide telecom fraud survey. Available: http://www.cfca.org/pdf/survey/2009%20Global%20Fraud%20Loss%20Survey-Press%20Release.pdf [accesses on 24 march 2010]", 2009

- CFCA, "Communication fraud control association results of worldwide telecom fraud survey. Available: http://www.cfca.org/pdf/press/3-28-06PR.pdf,[accesses on 24 March 2010]",2006

- CIFAS,the UK'S fraud prevention service," Fraud continues to leave a trail of damage. Available : http://www.cifas.org.uk/default.asp?edit_id=916-57, [accessed on 15 October 2010] ",2010

- Confidence group," phishing scams :understanding the latest trends trend You , a white paper presented by fraud watch internets high profile fraud prevention website available : http://www.fraudwatchinternational.com/pdf/report.pdf, [accessed on15 October 2010],"2004

- CR-C Transformation engine, "telecom fraud and fraud prevention, conference survey results, available: http://www.cr-x.com/downloads/CR-X_Fraud_Survey_Results_Singapore_2007.pdf ,[accesses on May 2010]", Singapore, 2007.

- D.estevez,c m.held,c a.preze ,"subscription fraud prevention in telecommunication using fuzzy rules and neural network, department of electrical engineering university of chilie, avilble: http://www.cec.uchile.cl/~pestevez/RI0.pdf ,[accessed on13 may 2010]",2005.

- D.Lioyd ,"fraudsters find a new frontier :wireless roaming, afire issac white paper, available: http://vip-cdg-wiki.qualcomm.com/w/images/6/6f/Fraud_WG_FairIsaacRoamingFraudWP.pdf ,[ accessed on 28 April 2010]," 2004

- Diticta, information inelegance," detecting telecoms subscription fraud", aDiticta white paper, available: WWW.Diticta .com, [accessed on 13 augest2009]", 2004

- element customer care, "new challenges in risk management, available: http://www.elementcare.com/documents/RiskManagementWhitepaper.pdf ,[accessed on 24 June 2010]",2008

- Enno Rey," Developing strategies to protect SS7 from manipulation and abuse, available:http://www.ernw.de/content/e7/e181/e1139/download1141/erey_ss7_security_v07_ger.pdf ,[accessed on13 November 2009]".

- Ernest and Young "the global fraud survey: fraud risk in the emerging markets. Technical report", 2006.

- F.chau ,"telecom fraud growing: survey, available: http://www.telecomasia.net/content/telecom-fraud-growing-survey-1, [accessed 21 march 2010]",2007

- Federal register,"Department of labor, Employment standard and administration wages and hour division" vol.73.no.28.avilable: http://www.dol.gov/whd/fmla/FedRegNPRM.pdf. [accessed on 25 October 2010]", 2008

- fierce wireless, " Juniper Research forecasts over 800 million consumers to use mobile banking services by 2011,fierce wireless, available: http://www.fiercewireless.com/press-releases/juniper-research-forecasts-over-800-million-consumers-use-mobile-banking-servic, [accessed on June 2,2010]",2008

- FOA Fiber optic association "what the jobs are, and how to find them, Available : http://www.thefoa.org/jobs/jobs.html ,[accessed on 8 June 2010" , 2010

- FSA, financial service authority," firms high –level management of fraud risk", available: http://www.fsa.gov.uk/pubs/other/fraud_risk.pdf , [accessed on 5 April 2010],"2006

- G.Bolongan,R.lindquist,"fraud auditing and forensic accounting,1995.Johwiley&son.newjersey

- Goliath business news, "why customer churn, available: http://goliath.ecnext.com/coms2/gi_0198-373341/4-Why-customers-churn.html,[accessed on 15 september2010]",2004.

- Grant Thornton," Trust and occupational fraud, how to trust is just as important as who to trust, white paper available:http://www.grantthornton.ca/resources/insights/white_papers/Trust_and_occupational_fraud_2010_electronic.pdf, [accessed on 15 April 2010]",2010

- GSM Association "Mobile Roaming Service in Latin America, Market &technical approach .IIRSA Workshop .Bogota, Colombia. Available: http://www.iirsa.org/BancoMedios/Documentos%20PDF/tir_bogota08_medidas_tecnicas.pdf , [accessed on 13 march 2009]",2008

- HR.Davia,P.Coggins.J.Widemen,J.kastintin,"accountant guide to fraud detections and control,2nd edition".2000. Johwiley&son.chaichtester,UK.

- Ict Qatar, "Bringing choice and quality service: mobile premium rate service available: http://www.ict.gov.qa/output/page1281.asp ,[accesses on13 June 2009]".

- Icta ,information and communication technology authority," Public consultation on indirect access ,available : http://www.icta.ky/docs/Indirect%20Access/CD(2003)7%20Indirect%20Access.pdf , [accessed on27 October 2010] ", 2003

- ISCE, institute for social and economic change, "stat macro-scan sms, INDIA, available: http://www.isec.ac.in/SMS%202010.pdf ,[accessed on15 May 2010]", 2010

- IUCN, the world conservation union," the IUCN anti-fraud policy, version 1, available: http://cmsdata.iucn.org/downloads/anti_fraud_policy.pdf ,[accessed on 22 June 2010] ", 2008

- J f ,Otero ,"revenue assurance and fraud. Caribbean telecoms briefing. Available: http://www.canto.co.cu/members/members_section/caribbean-telecoms-briefing/revenue-assurance-and-fraud , [accessed on19 December 2009]",2005

- J H V.Heerden ,[December 2005]," Detecting fraud in cellular telephone network" ,M S theses , in the –entire department ,program of operational analysis ,university of Stellenbosch ,south Africa , available: http://dip.sun.ac.za/~vuuren/Theses/vanHeerden.pdf ,[accessed on 14 June 2010] .

- J. Davey, "interconnect Node Location for voice calls originate on voice over next generation, awareness engagement & influence, available: http://www.btwholesale.com/pages/downloads/21_Century_Network_Community/c21_IP_016_040110_issue1.pdf ,[accessed on13 June 2010]", 2009

- J.Bayot " Ebbers sentenced to 25 year in prison for $11 Billion fraud. New York times .available : http://www.nytimes.com/2005/07/13/business/13WIRE-EBBERS.html, [accessed on16 December 2010]", 2005

- J.Hollmen.[Decemper.2000],"user profiling and classification for fraud detection in mobile communication networks" ,M S. thesis. Helsinki university of technology, available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.79.6058&rep=rep1&type=pdf," [accessed on 28 April 2010]".

- Javeline strategy & research, "Prepaid Fraud Mitigation: leveraging the processing Relationship to prevent fraud throughout the prepaid lifecycle, available: http://www.visadps.com/downloads/prepaid_fraud_mitigation.pdf, [accessed on13 may 2010] ", 2009

- k.Rabayah, S. Awad and N. A Kareem "Palestine ICT Market liberalization, Economic analysis an future Roadmap, available : http://www.pita.ps/newweb/pdfs/Palestinian_ICT_Market_Liberalization.pdf, [accessed on 19 June 2010 ]",2008

- KPMG," Uncovering fraud in the US companies, Uncovering fraud in the US companies. Available: http://www.cwu.edu/~holtfret/fraud_KPMG.pdf ,[accesses on 24 march 2010]", 1998

- KPMG, "India fraud survey report, available: http://www.in.kpmg.com/TL_Files/Pictures/Fraud_Survey_New.pdf , [accessed on 13 June 2010]", 2006

- KPMG," Revenue assurance in telecommunication progressing and preserving, global revenue assurance survey results, available: http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/Revenue , [accessed on13 December 2010]", 2009

- KROLL, "The Downturn and Fraud, your sector may even be better off available : http://www.kroll.com/about/library/fraud/Oct2009/downturn_and_fraud.aspx,[accessed 21October 2010]",2010

- Kroll,"Globla fraud report, economist intelligence unit survey result ,available: http://www.kroll.com/library/fraud/FraudReport_English-US_Oct10.pdf , [accessed on1 December 2010],"2010

- L.Allen," fraud and social engineering in community bank: information security trends and strategies ,available: http://www.larsonallen.com/Advisory_Services/Fraud_and_Social_Engineering_in_Community_Banks.aspx , [accessed on 20 November 2010]",2010

- L.cartodao,f.martins,a.rosa,p.caralho,"fraud management system in telecommunication :practical approach , available: http://www.telbit.pt/docs/ICT2005_FMS.pdf , [accessed on 15 august 2010]".

- M. Levi, J. Burrows, M.Fleming, M. Hopkins,k.Matthews "The nature, extend and economic impact of fraud in the UK,Report of the association of chief police officers, economic crime portfolio. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.108.8217&rep=rep1&type=pdf ,[accessed on 25th October 2010]",2007

- M.Gagnier "the rise and fall of Burnard L.Maoff .Blombirg Business week .available: http://www.businessweek.com/blogs/recession_in_america/archives/2008/12/the_rise_and_fa.html ,[accessed13 on October 2010]",2009

- M.Jans,N.Lybaret,k.Vanhoof ," a framework of internal fraud risk reduction at IT integrating business process ,international journal of digital accounting, the IFR farm work , available: http://www.uhu.es/ijdar/10.4192/1577-8517-v9_1.pdf ,[accessed on 13 March 2010]",2009

- M.Johneson, "Future fraud, telecom fraud in the next generation service.available:http://www.oct.ict.org/index.php?dir=4 ,[accessed on 28April 2010]," 2002

- M.Johnson ,"Revenues assurance, fraud &security in 3G service. Journal of economics and crime vol 1 issue 2, available: http://www.utica.edu/academic/institutes/ecii/publications/articles/BA2A7651-0488-EE3E-.pdf , [accessed on 13may 2010]",2002

- M.Kumar, T.grifinkel, D.bonen, T. winorad," reducing shoulder surfing by using gaze-password entry, Stanford University, available: http://www.stanford.edu/~talg/papers/SOUPS07/Eyepassword-soups07.pdf, [accessed on12 September]".

- MH Bihina Bella,MS Oliver,JHD Eloff," a fraud detection for the next generation, in D Brown (ed) Southern African network an application conference, available: http://mo.co.za/open/ngnfms.pdf , [accessed on15 June 2010]",2005

- N, Katzs.CFE.CFS ,"protect again procurement fraud" Inside supply management, vol .21,No.3 ,page 16.available: http://www.supplychainfraud.com/Katzscan%20ISM%20Procurement%20Fraud%20Article%20March%202010.pdf ,[ accessed on 23 July 2010]" ,2010

- N. kurtiz, "practical vision, securing a mobile telecommunication network from internal fraud, SANS institute reading room site, available http://www.sans.org/reading_room/whitepapers/wireless/securing-mobile-telecommunications-network-internal-fraud_166 ,[accesses on13 December 2009",2002.

- Namibia Economist, constitute of business inelegance "Anti fraud security under spotlight, available: http://www.economist.com.na/index.php?option=com_content&view=article&id=19341:anti-fraudtelecom-security-under-the-spotlight&catid=555:archives ,[accesses on 18 June 2010]",2005

- NAO National Audit Office "Good practice guide .tackling external fraud. available: http://www.nao.org.uk/guidance_and_good_practice/good_practice/idoc.ashx?docid=ed397377-07cd-40ae-88da-cda7fbe41131&ve , [accessed on 18 December 2009]",2008

- National fraud authority, "annual fraud indicator, available: http://www.attorneygeneral.gov.uk/nfa/GuidetoInformation/Documents/NFA_fraud_indicator.pdf, [accessed on june,2010] ",2010

- Nokia Siemens Network "Battling illegal call operations with Fraud Management Systems. Available: http://w3.nokiasiemensnetworks.com/NR/rdonlyres/3BEAAC03-80DF-40A4-8154-0E1001FBFAA7/0/Fraud_Management_white_paper.pdf, [accessed on January 2010]",2008

- Northwester,"long distance fraud warning affecting business with owned PBX system, available: http://www.nwtel.ca/media/documents/PBX-Toll%20Fraud.pdf , [accessed on13 November 2010] ".

- O A.Abidogun [august, 2005] ," fraud detection in mobile telecommunication "call pattern analysis with supervised neural networks, M A thesis, available: http://etd.uwc.ac.za/usrfiles/modules/etd/docs/etd_init_3937_1174040706.pdf ,[accessed on29 May 2009]".

- O.Nelsson [October, 2009] ,"Subscription fraud in telecommunication using detection tree learning" M .S. Thesis .Maker ere University, available: http://dspace.mak.ac.ug/bitstream/123456789/590/3/ojuka-nelson-cit-masters-report.pdf , [accessed on 28 April 2010]".

- P. Hale "The impact of bad debit on a company, available :http://EzineArticles.com/?expert=Patrick_H_Hale ,[accessed on 23 October 2010],"2010

- P. Hoath, "Fraud overview, TAF regional seminar on cost and tariffs , available: http://www.itu.int/ITU-D/finance/work-cost-tariffs/events/tariff-seminars/djibouti-08/Peter%20Hoath-4-EN.PDF , [accessed on 15 may 2009]",2008

- P.Pradhan ," mobile available: http://www.ntc.net.np/publication/smarika/smarika64/pratima_pradhan.pdfalu-added service roadmap , [accessed on18 November 2010]",2008

- P.thermos, ISSA, information system security association," Security behind the dial tone, countermeasures, and best practices, available: http://www.issa-centralva.org/presentations/2008/03-2008_pthermos_VoIP_Sec_Threats.pdf,[accessed on16 December 2009] ",2008

- PwC price whaterhuose of cooper, "Economic crime :people ,culture and the control, the 4th bi-ennial global economic crime survey. technical report"2007

- R G.Smith ,"Revenue Mobile Telephone Crime, Australasian institute of criminology , available: http://www.aic.gov.au/en/crime_types/economic/fraud/~/media/conferences/other/smith_russell/1996-10-crf.ashx ,[accessed on 12 December 2010].

- R G.smith," best practice in fraud prevention, Australian institute of criminology, trend and issues in criminal and justice ,available: http://www.aic.gov.au/documents/F/3/2/%7BF3256DEB-9A04-4416-9D11-156922F22EC8%7Dti100.pdf ,[accessed on13 September 2010]",1998

- R. Mathison ,"the revenue assurance standards" ,Global revenue assurance professional association GRAPA ,published by XIT PRESS okawa hills illions USA,2009, P-22.

- R.Doten ,"voice over IP security, Verizon business ,available:www.cscic.state.ny.us ,[accessed on15 October 2010]",2008

- R.kumar," fraud management system-selection and retuning ,unior, available: http://www.cerebralbusiness.com/telecom/presentations/Rajesh%20Kumar.pdf , [accessed on 13 December 2010]",2010

- R.Robert,D.Dabija "telecom fraud management training course" , Praesidium ,Qtel , 2009

- R.Shelton, "The Global Battle against Telecommunication Fraud. Available: www.satnac.org.za/proceedings/2003/plenary/Shelton.pdf , [accessed on13 march2010],"2003

- S k.doe," GSM roaming fraud, fraud in international roaming and fraud prevention techniques, available: http://www.ntc.net.np/publication/smarika/smarika64/sanjeeb_kumar_deo.pdf , [accessed on 13 September 2009]", 2008

- S N M .Noor, "international roaming in celecom Axita Berhad, international and demotic roaming, IUT ASO COE training workshop, available: http://www.itu.int/ITU-D/asp/CMS/ASP-CoE/2010/InterRoaming/session-7.pdf ,[accessed on10 august 2009]", 2010

- S. Grandhi,"application of data mining to credit card fraud,available: http://www.sas.com/offices/asiapacific/sp/usergroups/snug/archive/2010/presentations/SudhirGrandhiQ22010.pdf=, [accessed on 20 October 2010]",2010

- S. Thameem, slide share, "product assurance, Guide for product assurance risk and fraud assurance for all product and services lunched for telecom, available :http://www.slideshare.net/thamins/product-assurance-guideliness-for-yu , [accessed on 9 June 2010]".

- S.Brown ,"Telecommunication fraud management .available:http://waveroad.ca/ressources/Whitepaper_SB_Janvier2005.pdf, [accessed on23 December 2009],"2005

- Sanwalka, "Telecom fraud is the single biggest cause of revenue.availble:http://www.brighterion.com/PDFArticles/Telecomfraudisthesinglebiggestcauseofrevenueloss.pdf , [accessed on 15 October 2010] ",2010

- Sevis system, "Active fraud eliminator, minimize fraud from source such as illegal SIMBoxes(GSMGATWAYS).Available:http://www.sevis.com/root/media/Active_Fraud_Eliminator3.pdf ,[accessed on10 April 2010]".

- Softpedia, "telecom fraud not taken seriously by companies, available: http://news.softpedia.com/news/Telecom-Frauds-Not-Taken-Seriously-by-Companies-90939.shtml ,[accessed on 28 June 2010]", 2008

- Symsoft," Mobile &USSD, smart interactive service, available: http://www.symsoft.com/source.php/1279147/1002_Nobill_USSD.pdf , [accessed on 13 may 2010]", 2010

- T W .Hazeltt,: universal service telephone subsidies :what dos $7 Billion Buy? , available: http://www.senior.org/Documents/USF.Master.6.13.06.pdf , [accessed on15 October 2010]", 2006

- T.Chohen, R. Southwood, (2004), "An overview of VOIP regulation in Africa: Policy responses and proposals, for the commonwealth telecommunication s organization, available: http://www.cto.int/Portals/0/docs/voip_africa_overview.pdf, [accessed on 13 October]", 2010

- TRMG, the risk management group,"Understandig telecom fraud: the fundamentals of telecommunication fraud, what is it, why does it happen, and what does the future hold" 2008, from www.trmg.org

- Wesley Kenneth Wilhelm "the fraud management life cycle theory, Holistic Approach to fraud management, Journal of economic crime management .Vol 2,Issue2.available:http://www.utica.edu/academic/institutes/ecii/publications/articles/BA309CD2-01B6-DA6B-5F1DD7850BF6EE22.pdf,[accessed on 3 may2010]", 2004.

- www.myjawwal.ps

# Annexes

**Dear Sir/ Madam . . .**

**After greetings,**

The following questionnaire is a part from a study prepared by the researcher in order to have her master degree based on preventing fraud in the cell phone networks, and it is worthy to mention that it is applied, as a case of study, on the Palestinian communication cell phone company JAWWAL.

Your contribution in answering this questionnaire forms the main axis for achieving this study; reaching through it to the aspired scientific facts.

I assure that the information you are filling in the questionnaire will be used only for the benefit of the scientific research, Therefore; I hope your answers are clear and precise.

Best Regard's

**Researcher/ Hiyam Eltawashi**
**IU Gaza**

**Fist: Primary information:**

1-Department/section

A. Sales
B. Due collection
C. Anti fraud
D. Risk operation
E. Complaints
F. Dealers

2-Experience

A. Less than year
B. 1-3 years
C. 3-5 years
D. More than 5 years

3-Qualifications

A. Diploma
B. Bachelor's degree
C. Post graduate studies

4- Age Group

A. 20-30 years
B. 30-40 years
C. More than 40

**Second: Gaps, motivations, cracks leading to fraud:**

| **Paragraph** | **Select only one choice** |
|---|---|
| 1. The importance of the anti fraud department: | 1. Very important<br>2. Important<br>3. Natural<br>4. Not important |
| 2. The most important step of preventing fraud in the company is: | 1. The pre subscription step<br>2. The activation step<br>3. The fraud detection step<br>4. The Fraud prevention step |
| 3. The Fraud affects: | 1. The revenue and losses of the company<br>2. Reputation of the company<br>3. The quality of the provided services<br>4. All of the mentioned above |

| Paragraph | Select only one choice |
|---|---|
| 4. The main impact of fraud attacks on the company: | 1. A lot, causing financial losses<br>2. Few but serious<br>3. Moderate<br>4. familiar and normal |
| 5. Most of the fraud cases are Discovered through: | 1. Sales person accuracy'<br>2. Fraud management system<br>3. Billing reports<br>4. By chance |
| 6. The bad debits resulted from the fraud are: | 1. Normal<br>2. Worrisome<br>3. Require more auditing on the anti fraud.<br>4. Considered huge and should be taken in consideration |
| 7. The motivation that led the subscriber to fraud is: | 1. Bad experience<br>2. The subscriber inelegance and innovation<br>3. Monetary value<br>4. All of the mentioned above |
| 8. Fraud awareness in Jawwal company: | 1. There is a great level of awareness in all the departments of Jawwal.<br>2. There is partial awareness in particular sections and departments.<br>3. There is insignificant awareness<br>4. There is lack of awareness |
| 9. Jawwal employee is: | 1. Qualified enough to deal with fraud problems and fraudulent<br>2. Qualified but needs training in this field<br>3. In need for a specialized training in this field.<br>4. Doesn’t need to know the fraud prevention and detection mechanisms, as it is the duty of a particular section. |

| Paragraph | Select only one choice |
|---|---|
| 10. The sales personnel: | 1. Qualified and having sufficient knowledge of fraud problems<br>2. Qualified but they focus on sales<br>3. Not qualified<br>4. Flexible with fraud cases in a negative way. |
| 11. The number of the discovered cases, sorted as fraud cases are: | 1. Rare<br>2. Few and refer to the anti fraud efficiency<br>3. Moderate and refer to improving anti fraud<br>4. Numerous and refer to the need for More efficient anti fraud tools |
| 12. The insolvent customer differs from fraudulent customer in: | 1. Had no previous intention to defraud<br>2. Committed with the company for a long time<br>3. Possibility to pay the due amounts<br>4. All of the mentioned above |
| 13. The fraudulent customer: | 1. Had pervious intention to defraud ate<br>2. Had a bad experience with the company led to defraud.<br>3. Utilize the system gaps<br>4. All of the mentioned above |
| 14. The customer is considered fraudulent if: | 1. Had the intention to defraud ate<br>2. Illegally used the company services<br>3. Used faked documents<br>4. All of the mentioned above |
| 15. The current criteria to identify the fraudulent are: | 1. Efficient and lead to discover all of the fraud customers.<br>2. Efficient but being relativity makes the fraud attacks possible.<br>3. Needs more effective criteria.<br>4. Inefficient and can’t prove that the customer is fraudulent. |

| Paragraph | Select only one choice |
|---|---|
| 16. The anti fraud employee can identify the fraudulent customer through: | 1. The sudden change in his usage (calls/services).<br>2. Kinds of the requested services.<br>3. The number of the requested lines, and his discharge.<br>4. All of the mentioned above |
| 17. Targeting sales is consider one of the factors that increase the fraud attacks through: | 1. Focusing on the number of the sold lines but not the quality of the service.<br>2. Working under pressure.<br>3. The employee's negligence in disconnecting the suspected subscriptions.<br>4. All of the mentioned above. |
| 18. The dealers are considered a window for fraud attacks through : | 1. Having separate aims away of the company's aims.<br>2. Insufficient knowledge about fraud problems.<br>3. Absence of procedures and rules that focus on fraud problem.<br>4. All of the mentioned above. |
| 19. Working policies and procedures are: | 1. Clear about fraud problem.<br>2. Unclear and includes gabs.<br>3. Unclear and incomprehensive.<br>4. Unclear and need to be modified. |
| 20. The accelerate modifying of policies and procedures is: | 1. Useful and serve work<br>2. Useful but needs to be at low rate of speed.<br>3. Useful but squanders the employee attention.<br>4. Un-useful and doesn't serve the work. |

| Paragraph | Select only one choice |
|---|---|
| 21. Promotions and campaigns are: | 1. Comprehensive and accurate.<br>2. Skillful but contains gaps to defraud company.<br>3. Not examined and there is gaps to defraud ate the company.<br>4. They are not consider window to defraud ate. |
| 22. Current fraud detection tools are: | 1. Comprehensive and reliable<br>2. Needs more efficient tools to prevent defraud<br>3. Efficient but doesn't prevent defraud ate.<br>4. one efficient tool will be more accurate |
| 23. The fraud management system is: | 1. Comprehensive and reliable<br>2. Reliable but can't discover all the defraud situations.<br>3. Needs update and modification<br>4. Inefficient, Jawwal needs to employ new program. |
| 24. Billing reports are: | 1. Essential tool to fraud detection.<br>2. Supportive tool to fraud detection.<br>3. Supportive but not useful.<br>4. Not reliable tool to depend on for detecting fraud. |
| 25. The black list window is : | 1. Comprehensive data base to discover the black listed customers.<br>2. Comprehensive data base but not sufficient to discover all the black listed customers.<br>3. Needs modification.<br>4. Not efficient toll to discover the black listed customers. |

| Paragraph | Select only one choice |
|---|---|
| 26. information concerning with defraud attacks from another sources such as: (complaints-call center-sales-provisioning) are: | 1. Efficient source to discover all the fraud cases.<br>2. Efficient source to discover some of the qualitative fraud cases.<br>3. Subordinate source.<br>4. Inefficient source. |
| 27. The required documents for the new superscription applications and agreements are: | 1. Comprehensive.<br>2. Comprehensive and can't be exceeded.<br>3. Not comprehensive.<br>4. Needs to be stricter. |
| 28. The services activated by default are: | 1. Increase the company vulnerability to fraud.<br>2. Good and useful for the customer.<br>3. Need to be stricter.<br>4. They are not related to fraud attacks. |
| 29. The insurance policy is: | 1. Suitable.<br>2. Good cover in case the customer became fraudulent.<br>3. Suitable but needs to be modified.<br>4. Unsuitable for all the customers. |
| 30. The pricing policy is : | 1. Suitable and not considered a motive to defraud ate the company.<br>2. High.<br>3. Moderate.<br>4. Unsuitable and is considered a motive to defraud ate the company. |
| 31. The most vulnerable service to the fraud attacks is the: | 1. International roaming.<br>2. International.<br>3. Short message service.<br>4. Wap and internet. |

| **Paragraph** | **Select only one choice** |
|---|---|
| 32. The increscent of fraud attacks in the Gaza region is due to: | 1. The current bad economical and political conditions.<br>2. The customer innovation<br>3. Acquiring the sales target instead of the service quality<br>4. All of the mentioned above |
| 33. The increscent of fraud attacks in the corporate system is due to: | 1. The corporate sales policy and the absence of guarantee on most of the activated lines.<br>2. Sales target.<br>3. Activating some services such as ID and IR without any guarantee.<br>4. All of the mentioned above. |
| 34. The most efficient way to detect fraud is : | 1. Centralizing the anti fraud tasks<br>2. establishing anti fraud section in every related department<br>3. Expanding the current anti fraud section authorities<br>4. Fraud can't be avoided |
| 35. Collaborative efforts between some destinations like (Paltel., banks, ministry of interior affairs) are : | 1. Very useful<br>2. Useful and can help in minimizing the fraud losses<br>3. Useful but not applicable<br>4. Useless efforts |

بسم الله الرحمن الرحيم

**أختي الكريمة / أخي الكريم:**

**السلام عليكم ورحمة الله وبركاته،،،،**

الاستبانه المرفقة جزء من دراسة تعدها الباحثة لنيل درجة الماجستير حول منع التحايل في شبكات الهواتف الخلوية وطبقت على شركة الاتصالات الخليوية الفلسطينية جوال , كحاله للدراسة, مساهمتكم في الإجابة عن أسئلة الاستبانه تمثل المحور الأساس لانجاز هذه الدراسة ووصولها للحقائق العلمية المرجوة.

لذا آمل منكم الإجابة عن أسئلة هذه الاستبانه بكل دقة ووضوح, وأؤكد لكم بأن البيانات التي ستدلون بها في الاستبانه لن تستخدم إلا لغرض البحث العلمي فقط.

مع تمنياتي بالتوفيق لكم

**الباحثة/ هيام الطواشي**
**الجامعة الإسلامية-غزة**

1- **الدائرة/ القسم:**

أ- المبيعات

ب- التحصيلات السابقة

ج- منع التحايل

د- عمليات المخاطرة

ه- الشكاوي

و- الموزعين والوكلاء

ز- علاقات وخدمات المشتركين

2- **الخبرة:**

أ- أقل من سنة

ب- 1- 3 سنوات

ج- 3-5 سنوات

د- 5 فأكثر

3- **المؤهل العلمي:**

أ- دبلوم

ب- بكالوريس

ج- دراسات عليا

4- **الفئة العمرية:**

أ- 20- 30 سنة

ب- 30- 40 سنة

ج- أكبر من 40

**ثانيا: المنافذ والعوامل المهيئة للاحتيال:**

| فقرة | البدائل (الرجاء اختيار بديل واحد فقط) |
|---|---|
| 1- أهمية جهود قسم منع التحايل: | أ- مهمة جداً<br>ب-مهمة<br>ج- عادية<br>د- غير مهمة |
| 2- أهم مراحل منع التحايل على الشركة: | أ- مرحلة ما قبل الاشتراك (قبل دخول المشترك المتحايل إلى الشبكة)<br>ب-مرحلة تفعيل الخدمة (مرحلة التدقيق)<br>ج- مرحلة اكتشاف حالات التحايل<br>د- مرحلة تطبيق إجراءات منع التحايل |
| 3- يؤثر التحايل على: | أ- أرباح وخسائر الشركة<br>ب-سمعة الشركة لدى الجمهور<br>ج- جودة الخدمة المقدمة<br>د- جميع ما سبق |
| 4- هجمات التحايل التي تتعرض لها الشركة: | أ- كثيرة وتؤدي إلى خسائر مالية<br>ب-قليلة في العدد ولكنها نوعية خطيرة<br>ج- متوسطة وغير نوعية<br>د- عادية ومألوفة |
| 5- معظم حالات التحايل يتم الكشف عنها من خلال: | أ- دقة موظف المبيعات<br>ب-برنامج منع التحايل<br>ج- تقارير الفوترة<br>د- بالصدفة |
| 6- قيم الديون المعدومة الناتجة من حالات التحايل: | أ- طبيعية وغير مقلقلة<br>ب- غير طبيعية ومقلقة<br>ج- تستدعي التدقيق أكثر على موضوع منع التحايل<br>د- كبيرة وبحاجة إلى إعادة النظر في أداء منع التحايل |
| 7- من الدوافع التي تؤدي بالمشترك الاحتيال على الشركة: | أ- موقف مسبق من الشركة<br>ب-تفوق المتحايل وابتكاره لأساليب جديدة لا يعلم بها موظف منع التحايل<br>ج- الاستفادة المادية مثل إعادة بيع الخطوط<br>د- جميع ما سبق |

| فقرة | البدائل (الرجاء اختيار بديل واحد فقط) |
|---|---|
| 8- الوعي بمشكلة التحايل في داخل الشركة: | أ- يوجد وعي لدى جميع الدوائر والأقسام بمدى خطورة مشكلة التحايل<br>ب-يوجد وعي ولكن لدى أقسام معينة على اعتبار أنها متخصصة في التعامل مع المشتركين<br>ج- لا يوجد وعي كافي بمشكلة التحايل لدى الشركة<br>د- لا يوجد وعي إطلاقاً بمشكلة التحايل |
| 9- موظف شركة جوال: | أ- مؤهل جداً للكشف والتعامل مع المشترك المتحايل<br>ب-مؤهل ولكن ينقصه التدريب بهذا المجال<br>ج- بحاجة إلى تدريب متخصص في هذا المجال<br>د- ليس بحاجة إلى الاطلاع على قضية التحايل على اعتبار أنه موضوع يخص قسم معين |
| 10- موظفي المبيعات: | أ- لديهم الخبرة والمهارة الكافية للتعامل معه مشكلة التحايل<br>ب-لديهم الخبرة والمهارة الكافية ولكن التركيز على الهدف البيعي فقط<br>ج-ليس لديهم الخبرة المطلوبة للكشف عن المشترك المتحايل<br>د- يتهاونون في قبول بعض الحالات ويتساهلون مع معارفهم من الزبائن |
| 11-عدد الحالات التي يتم الكشف عنها وتصنف على أنها حالات تحايل: | أ- نادرة<br>ب-قليلة وهي مؤشر جيد على كفائة الأساليب المتبعة لمنع التحايل<br>ج-متوسطة وهي مؤشر لحاجة الشركة إلى تطوير بعض أدوات منع التحايل<br>د- كبيرة وتعتبر مؤشر لحاجة الشركة إلى أدوات أكثر فعالية |
| 12-المشترك المتعثر ماليا يختلف عن المشترك المتحايل من حيث: | أ- عدم وجود النية المسبقة للتحايل على الشركة<br>ب-التزامه لفترات طويلة مع الشركة<br>ج- إمكانية تحصيل المبالغ المتراكمة<br>د- جميع ما سبق |
| 13-المشترك المتحايل هو شخص: | أ- لديه النية المسبقة للتحايل على الشركة<br>ب-تعرض لموقف أدى به للتحايل على الشركة(شكوى لم تحل- ارتفاع أسعار)<br>ج- استغل ثغرات موجودة في نظام الشركة<br>د- جميع ما سيق |

| فقرة | البدائل (الرجاء اختيار بديل واحد فقط) |
|---|---|
| 14-يعتبر المشترك متحايل إذا: | أ- شخص لديه النية للتحايل<br>ب- استخدم خدمات الشركة بطريقة غير مشروعة<br>ج- زور في أوراقه الثبوتية<br>د- جميع ما سبق |
| 15-المعايير الحالية لكون المشترك متحايل: | أ- فعالة وتؤدى إلى الكشف عن كل حالات التحايل<br>ب- فعالة ولكن كونها معايير نسبية تجعل الباب مفتوحا لنفاذ بعض حالات التحايل<br>ج- بحاجة إلى معايير أكثر شموليه<br>د- غير فعالة ولا تستطيع الجزم بكون المشترك متحايل |
| 16-يستطيع موظف منع التحايل تحديد المشترك المتحايل من خلال: | أ- تغيير نمط استهلاكه لبعض الخدمات وارتفاع معدل مكالماته<br>ب- نوعية الخدمات التي يطلبها<br>ج- عدد الخطوط التي يستخدمها ومعدل تسديداته<br>د- جميع ما سبق |
| 17-يعد الهدف البيعي عامل في زيادة حالات التحايل على الشركة من خلال: | أ- التركيز على عدد الخطوط المباعة وليس على جودة الخدمة<br>ب- ضغط العمل يؤثر على تركيز ودقة الموظف<br>ج- تهاون الموظف في توقيف بعض الاشتراكات التي يشك في دقتها<br>د- جميع ما سبق |
| 18-يشكل الوكلاء والموزعين منفذ للتحايل من خلال: | أ- بُعد أهداف الموزعين والوكلاء عن أهداف الشركة<br>ب- عدم إطلاع الموزعين والوكلاء على موضوع التحايل<br>ج- آليات العمل المتعلقة الموزعين والوكلاء لم تسلط الضوء على مشكلة التحايل وكيفية التعامل معها<br>د- جميع ما سبق |
| 19-آليات وسياسات العمل: | أ- واضحة في التعامل مع المشترك المتحايل<br>ب- واضحة ولكن بها منافذ يستطيع المشترك المتحايل استغلالها.<br>ج- غير واضحة ولا تشمل جميع الحالات<br>د- غير واضحة وبحاجة إلى إعادة النظر فيها |
| 20-التغيير المتسارع للآليات والسياسات: | أ- نافع ومفيد ويخدم مصلحة العمل<br>ب- نافع ومفيد ويجب أن لا يتم بشكل متسارع<br>ج- جيد ولكن يودي إلى تشتيت الموظف<br>د- غير جيد ولا يخدم العمل بالصورة المطلوبة |

| فقرة | البدائل (الرجاء اختيار بديل واحد فقط) |
|---|---|
| 21-الحملات والعروض: | أ- شاملة ومتكاملة لا يستطيع المشترك إيجاد ثغرات فيها<br>ب-معدة بشكل جيد ولكن يوجد بها منافد للتحايل<br>ج- عير مفحوصة ومختبرة بشكل جيد وبها منافد للتحايل<br>د- الحملات والعروض لا تشكل منفذ للتحايل |
| 22-أدوات التحايل المستخدمة حاليا: | أ- شاملة وتستطيع الشركة الاعتماد عليها لمنع التحايل<br>ب-بحاجة أدوات أكثر فعالية لمنع التحايل<br>ج- جيدة ولكنها لا تمنع التحايل بفعالية<br>د- يفضل وجود أداة موحدة وفعالة تغني الموظف من البحث في كل تلك المصادر |
| 23-برنامج منع التحايل (FMS) : | أ- فعال ويستطيع الكشف عن كل حالات التحايل<br>ب-جيد ولكن لا يستطيع الكشف عن كل حالات التحايل<br>ج- بحاجة إلى تطوير وتعديل ليصبح أكثر فعالية<br>د- غير فعال والشركة بحاجة إلى اعتماد برنامج آخر |
| 24-تقارير الفوترة: | أ- أداة رئيسية للكشف عن جميع حالات التحايل<br>ب-أداة مساعدة بجانب برنامج منع التحايل ولكنها تحتاج للكثير من الوقت والجهد<br>ج- أداة جيدة ولكنها ليست الوسيلة الناجحة لمنع التحايل<br>د- أداة غير فعالة لاعتمادها كوسيلة لمنع التحايل |
| 25-برنامج القائمة السوداء، الأهم في فحص المشترك المتحايل وهو: | أ- قاعدة بيانات شاملة وفعالة للكشف عن المشترك المتحايل<br>ب-قاعدة بيانات ولكنها غير فعالة للكشف عن جميع حالات التحايل<br>ج- بحاجة إلى تعديل أكثر ليصبح أكثر فعالية<br>د- غير فعال للكشف عن المشترك المتحايل |
| 26-المعلومات عن وجود حالات تحايل من مصادر أخرى مثل(الشكاوي - الخدمات - مركز الاستعلامات- المبيعات) هي: | أ- مصدر فعال جدا للكشف عن جميع حالات التحايل ويجب تفعيل دوره<br>ب-مصدر جيد للكشف عن بعض حالات التحايل النوعية<br>ج- مصدر مساعد ولكنه غير أساسي وغير محكوم باليات وسياسات عمل<br>د- مصدر غير فعال للكشف عن حالات التحايل |
| 27-الوثائق المطلوبة في طلبات الاشتراك والاتفاقيات الجديدة: | أ- كافية وشاملة لتسليط الضوء على المشترك المتحايل<br>ب-كافية ولكن يستطيع المشترك تجاوزها وإيجاد ثغرات فيها<br>ج- غير كافية<br>د- بحاجة لوضع قيود أكثر على طلبات الاشتراك |

| البدائل (الرجاء اختيار بديل واحد فقط) | فقرة |
|---|---|
| أ- تزيد من تعرض الشركة للتحايل مثل خدمة الرسائل القصيرة<br>ب- جيدة ونافعة للمشترك والشركة<br>ج- بحاجة لوضع بعض القيود على تفعيل تلك الخدمات<br>د- لا علاقة لتلك الخدمات بموضوع التحايل | 28-الخدمات التي يتم تفعيلها بشكل تلقائي للمشتركين: |
| أ- مناسبة جدا<br>ب- تعتبر غطاء جيد في حال أصبح المشترك متحايل<br>ج- مناسبة ولكنها بحاجة للتعديل<br>د- غير مناسبة لجميع المشتركين | 29-سياسة التأمينات في الشركة: |
| أ- مناسبة لجميع المشتركين ولا تخلق دافع للتحايل<br>ب- مرتفعة<br>ج- متوسطة<br>د- غير مناسبة وتشكل دافع للتحايل | 30-أسعار الخدمات المعتمدة لدى الشركة : |
| أ- التجوال الدولي<br>ب- الصفر الدولي<br>ج- الرسائل<br>د- الواب والانترنت | 31-من أكثر الخدمات خطورة وعرضة للتحايل: |
| أ- الوضع الاقتصادي والسياسي القائم<br>ب- إبداع وابتكار المشترك المتحايل من منطقة غزة<br>ج- تحقيق الأهداف البيعية الكبيرة دون التركيز على جودة الخدمة<br>د- جميع ما سبق | 32-ازدياد حالات التحايل في منطقة غزة عائد إلى: |
| أ- سياسة الشركات البيعية وعدم وجود تأمينات على جميع الخطوط<br>ب- عدم وجود قيود على عدد الخطوط الممنوحة<br>ج- تفعيل بعض الخدمات مثل الصفر الدولي والتجوال الدولي دون وجود تأمينات<br>د- جميع ما سبق | 33-ارتفاع حالات التحايل في نظام الشركات نتيجة لـــ: |

| فقرة | البدائل (الرجاء اختيار بديل واحد فقط) |
|---|---|
| 34-الطريقة الأمثل لمنع التحايل: | أ- تركيز وجود منع التحايل في وحدة واحدة تحت إدارة العناية بالزبائن<br>ب-وجود أكثر من وحدة لمتابعة التحايل في كل قسم<br>ج-تعميم وجود قسم موحد له تأثير أكبر على جميع أقسام الشركة<br>د- التحايل موجود ومشكلة لا يمكن تلاشيها |
| 35-إيجاد تعاون مشترك بين جهات ذات علاقة مثل)بالتل-البنوك-وزارة الداخلية ) هي جهود: | أ- فعالة جدا<br>ب-جيدة ولها تأثير ايجابي للحد من التحايل<br>ج- جيدة ولكنها صعبة التطبيق<br>د- لن تؤتي بالجهد المطلوب للحد من التحايل |

الجامعة الإسلامية – غزة
عمادة الدراسات العليا
كلية التجارة
قسم إدارة الأعمال

# منع التحايل في شبكات الهواتف الخلوية

## دراسة حالة (شركة جوال)

عمل الطالبة

**هيام علي الطواشي**

إشراف

**أ. د. يوسف حسين عاشور**

“A Thesis Presented in Partial Fulfillment of the Requirement for the Degree in "MBA"

أغسطس 2010