



"THE FORUM OF TRUST"

IN THE FRAME

THE REGULAR TUFF NEWSLETTER
PUBLISHED QUARTERLY



VOLUME 10 ISSUE 1

APRIL, MAY & JUNE
2008

ON THIS PAGE

VQ's First Success

Seminar 2008

INSIDE THIS ISSUE

Accreditation Results 2

Catching The Thief! 2

Fraud In The Retail Environment 3

Dr Fraud

Do You Speak Japanese? 4

TUFF VOCATIONAL QUALIFICATION



June AGM was a special occasion in that it saw the first award of a TUFF VQ Certificate to the first student to complete the full VQ course. **Shona Moore** is seen here getting her certificate from the Chairman of TUFF, **Louis Groves** of BT. In presenting the award Louis highlighted the work that had been done by Shona to achieve this "First".

In addition to completing the 4 compulsory workshops covering Legislation, Analysis and Information Sharing, Fraud Department Organisation and Report Writing Shona also completed a 3,500 word article on "Is it socially acceptable to make a fraudulent insurance claim for a mobile phone" a critical look at the problems associated with insurance and mobile phone fraud. Shona also attended 2 of the TUFF Training days to qualify for additional points. Any reader who is interested in following Shona's footsteps can contact Nevilline Barretto at the TUFF General Office for details on how to become registered for the VQ course of study.- nbarretto@tuff.co.uk

NEURAL TECHNOLOGIES SPONSORED TUFF ANNUAL SEMINAR AND AWARDS EVENING 2nd & 3rd September 2008



Tuesday the 2nd and Wednesday the 3rd of September will see the Forum members coming together to attend the annual seminar and awards evening. The Seminar, sponsored this year by **Neural Technologies**, is beginning to take shape with confirmed presentations and workshops from a number of leading industry figures and details will be posted out to members in July along with a posting on the TUFF web site. Members who have

attended in previous years will need no encouragement to attend the evening awards ceremony which is an informal gathering of members and their friends to honour those individuals and organisations who have done their bit to further the fight against fraud and crime within the telecommunications industry. Nomination forms for a TUFF Award are available from the TUFF General Office and have to be returned completed by 7th August 2008. If for some reason you are unable to obtain a nomination form then a short email describing the background to a nomination will suffice and should be sent to the CEO at tuff@tuff.co.uk with the subject line **Nomination For an Award.**



How Phones 4U Caught “Marlon the Mighty”

(This article was submitted by Herinder S. Bassi, Operational Intelligence Analyst, Phones 4U)

Richard Thomas and Mark Walport recently completed their review of data sharing within the United Kingdom.

The review was brought about by the headline cases of data loss in the latter half of 2007 and early 2008.

The full report which runs to some 80 pages and is available at:-

www.justice.gov.uk/re-views/datasharing-intro.htm

The most important recommendation in the report calls for a “**significant improvement in the personal and organisational culture of those who collect, manage and share personal data**”

In the last few decades there has been a major improvement in governance in the commercial, charity and voluntary sectors. However, in many organisations the governance of the handling of personal information has not followed suit. The report was published on the 11th July 2008.

Starting in July 2007 a distinctive spate of store thefts and attempts occurred. Intelligence Analysts at Phones4u produced a Problem Profile in response to this threat. This Intelligence



Product is derived from the National Intelligence Model (NIM), as developed by Law Enforcement Agencies. The Problem Profile was disseminated to TUFF, the conduit for our telecommunications industry partners. Intelligence Dissemination is a cornerstone of Best Practice without it valuable resources can be ultimately made redundant. TUFF facilitated the further sharing of the Intelligence as the issue impacted on all mobile phone partners. The profile identified an Offender Description and Method of Operandi (MO), which was to **steal a dummy handset from one retailer and proceed to the next**

Do You Know This Guy? where he would swap the dummy for a real handset being demonstrated. Temporal and geographical analysis identified the offending pattern from the London area to the Midlands and Scotland, very much a cross border police problem. Over 50 incidents were collated including nearly 30 thefts from Phones 4U. The offender took on a cult type status and was nicknamed “**Marlon The Mighty**”! He was arrested on three separate occasions, in Birmingham, Harrow and Uxbridge. Stolen property recovered included Carphone Warehouse stock. However when bailed his chaotic offending continued.

Sharing this information had fantastic results, as the alerted neighbouring retailers assisted in the final arrest.

Our investigators cornered and detained him in Glasgow. As he was a prolific persistent offender and not domiciled in the UK, he is currently detained with a view to deportation.

The success of this multi agency approach and intelligence sharing meant the shared threat was tackled in partnership with a good goal achieved by the TUFF team.

CONGRATULATIONS

THE FOLLOWING MEMBERS ALL HAVE TAKEN ACCREDITATION EXAMS THIS YEAR AND BEEN AWARDED THEIR ACCREDITATION CERTIFICATES WELL DONE!

(The next Accreditation examinations are due to be held next on the 2nd October in Birmingham, although if member companies have more than 3 candidates examinations can be arranged on their own premises)

John	Fothergill	Phones4U
Mark	Griffin	Phones4U
Anthony	Navaie-Bryan	Phones4U
Kevin	Fitzgerald	Phones4U
Dawn	Ramsay	Phones4U
Lynsey	Cochrane	Phones4U
Will	Richards	Subex ***
Mark	West	Subex
Sonia	Hassanali	CPW
Katherine	Hudson	CPW
Sara	Dobson	CPW ***

*** = Indicates Distinction on Both Papers—Very well done

INITIATIVES TO TACKLE FRAUD IN THE RETAIL ENVIRONMENT



When a customer calls to report that they have had their name/address/bank details used, they are asked for their permission to pass the details to the Security system of **Phones 4U**. When permission is given, the details are loaded onto a database, with checks real time applications made in Phones 4U outlets. This gives us visibility of potentially fraudulent transactions whilst the fraudster is standing at our tills.

The process that we follow is simple. If any part of a new sale matches any data loaded onto the security system, then the security team are alerted. Security can then quickly call the customer to clarify whether or not they are in the store, If they say yes, then the sale will go ahead as normal.

If they say no – then we know that we have a fraudster in store! From this point, the police are called and hopefully the offender will be apprehended in store. Sometimes the fraudster becomes suspicious and leaves - But what happens then? They probably go to **Carphone, Vodafone** or another telecoms store on the high street. If they haven't hit that retailer before – they could walk away with another couple of fraudulently obtained contracts. The transfer of this data to Phones 4U within days of the inception enables the information to help fight fraud and assist prevention not only for Phone 4U but by exchanging this with other TUFF members the wider telecommunication community before they are targeted.

The key message is information sharing. Identity fraud reports invariably means reacting to a situation – If we all information share – then we can be more proactive in protecting our businesses and reputation. TUFF provides the right environment to facilitate this.

(This article is the work of Lori Hunter an Analyst with Phone 4U and is part of her course of study for her TUFF Vocational Qualification)



Dear Doctor Fraud



Dear Doctor Fraud,

Recently I have read of companies being taken over by fraudsters who then go on to commit fraud in the newly acquired company's name. Is there anyway I can guard against this sort of thing happening to me?

R U Swift

Dear R,
first let me say that you are right to be worried. There has been a significant increase of late in this type of takeover of companies and a lot of the time the take over has enabled fraudsters to run up bills and other charges against the real unsuspecting company. The problem has been highlighted by Companies

House who have now introduced a new service which enables companies who are concerned to register to be informed whenever documents are filed at Companies House against their company. Full details of this and other services are now available on the Company House web site at www.companieshouse.gov.uk/index.shtml
Dr Fraud

WHAT IS IN A NAME? "WHALING"

A New Form of Phishing!

What is unique about whaling is its reliance on research and social engineering.

Traditionally spam, and to some extent phishing, depends on reaching the greatest number of people with the smallest amount of effort, considering the response rate to these e-mail abuses tends to be miniscule but still enough to make the practice worth it.

With whaling, the sender must do some upfront research about the target

as well as the subject in order to craft an e-mail that sounds convincing.

"It's really the social engineering that has tipped the balance now; phishers are becoming much more technologically sophisticated as well as applying psychology to what they're doing, Now they conduct a lot of research before they attack, so it becomes much more difficult to recognize those attacks." Full report is at:

www.networkworld.com/news/2007/111407-whaling.html

Wangiri - A Lesson In Japanese?



(With Thanks to Neural Technologies Fraud & Revenue Focus Newsletter *)



A growing trend in Premium Rate Services (PRS) and Personal Number Service (PNS) abuse takes the form of a scam known as Wangiri. The term derives from Japan where the scam is believed to originate and it literally means

‘one ring and cut’.

So how does it work?

A computer is used to dial mobile phone numbers, either at random or in blocks. The call disconnects before the subscriber answers and a missed call notification appears on the recipient's mobile. The intention is to encourage the subscriber to return the call. What the subscriber doesn't realise is that the numbers used are either premium rated and/or contain long advertising messages. In many instances the number is changed to represent a national number to hide the fact that a premium rate number is being used.

A typical bogus voicemail message received on calling back these numbers is *“Sorry, the person you are calling is temporarily unavailable”*, or *“Attempting to connect you please wait”*, then after 40 seconds or so this changes to *“Sorry leave a message”*.

UK operators have reported that in a typical weekend there are over 10,000 returned calls to these PRS or PNS numbers. One operator's customers experienced a costly variation of the fraud where, instead of PRS numbers being used, the originating calls were from satellite numbers. For the fraudster this type of scam is a low-cost way of inflating PRS and PNS revenues:

- There is no charge for an unsuccessful call
- There is minimal charge if the call goes to voicemail
- More revenue can be secured via the use of long recorded messages or recorded ring tones.

How to detect and prevent Wangiri Fraud

So what can be done to detect and prevent Wangiri Fraud? Firstly it is crucial to gain Network Operations' involvement to assist in analysing traffic patterns on the network. They will be able to identify wrong call types, unsuccessful network clear codes or any congestion. In addition Customer Services can collate and monitor customer queries or complaints and also provide customer awareness information. Once Wangiri fraud has been detected, you should attempt to contact the number range owner to stop the traffic. If events continue then bar the incoming range on interconnect MSC. Where possible withhold interconnect charges (AIT process).

For operators who are using Neural Technologies' Minotaur™ solution, a series of rules can be created to identify the fraud based on the calling patterns which typically involve:

- **A high volume of incoming events from 90xx ranges (070xx as well if UK)**
- **A high volume of calls from same incoming number ranges**
- **Incoming calls to sequential or distinct numbers**
- **Distinct (all different A numbers) calls to same PRS numbers**
- **Calls to PRS numbers within a range**
- **Calls to numbers not in service**

The impact of Wangiri fraud

Whilst there is generally no monetary loss to the operator, this kind of fraud causes increased customer complaints, negative PR and the risk of churn. Reported customer complaints received to date include:

- **The service was not advertised on the Internet or in any literature**
- **Customers had no ability to opt in or opt out of the service**
- **No notification of cost (average cost \$2 per minute)**
- **Any number can be targeted e.g. VIPs**

Operators must be seen to be proactive as there has been a lot of recent media interest in PRS abuse. As this fraud trend develops, understanding Wangiri fraud and monitoring for it will be a key step towards protecting and retaining your customers.

* - www.neuralt.com/telecommunications.html