

fraud & revenue focus

1 Company News:

Nt Celebrates Award Win



2 Risk Focus:

New Trends in Internal Fraud



3 New Initiative:

Fraud and RA Workshops



4 Online Seminar:

Managing Dealer Fraud



5 Customer News:

Orange and Trilogy Go Live



Winner: Large Technology Supplier of the Year

Neural Technologies has been named Large Technology Supplier of the Year by the British Computer Society (BCS).

The company was presented with an Organisational Excellence Award for its ground-breaking work with DirecTV, the US's leading digital TV entertainment provider. The project represented the first fraud implementation within the direct broadcast satellite industry in North America.

The company beat off competition from industry giants such as Sun Microsystems, IBM, Ericsson, and EMC² to win the sought after award which recognises excellence and innovation in IT.

James Whalen, Vice President of Signal Integrity within DirecTV said, "A well deserved award as you are truly a remarkable company who puts its customers first. You are not only a first class vendor, you are an exceptional team who went above and beyond the contract to support the implementation of DirecTV's Fraud Management System. We couldn't be prouder of your achievement, as evidenced by the BCS IT Industry Award, and look forward to our long term relationship. All of you who contributed to this award are simply put 'awesome' and it validates once again our choice of Neural Technologies as our fraud management system vendor".



About the British Computer Society Awards

The British Computer Society (BCS) has been recognising outstanding achievement in IT for over 30 years through its annual awards, which are a leading hallmark of success amongst practitioners in the IT industry today. The awards recognise and promote excellence, professionalism, innovation and the outstanding achievements to which individuals and groups contribute. Said Alan Pollard, BCS president, "The standard of entry has been exceptionally high this year and the judges faced a daunting task to select those that had that something extra. Each year the quality of entrants and the standard of submissions seem to outshine the previous and everyone taking part this time can feel justifiably proud of their work".

Message from the CEO



John Gavan
John Gavan CEO
Neural Technologies

Speculation continues that a further round of mergers and takeovers is set to begin in the telco arena. Operators, both fixed and mobile, are seen by many as "safe haven" investments in the maturing markets and "sound growth" in emerging markets. Coping with the challenges that these events bring is sometimes not easy. Fraud and bad debt often rises, sometimes dramatically during this time. Increasingly Neural Technologies is being called in post-merger to help reduce these risks and we have a number of newly-signed contracts addressing these very issues.

Continuing with the mergers and acquisition theme, I am delighted to announce that Neural Technologies has taken a controlling interest in one of Hong Kong's most successful telephone software specialists. They provide many of the largest operators in the region with advanced applications for handsets, intelligent networks and virtual mobile networks. More details in our next issue.

Finally, I must take this opportunity of saluting the team that was so successful in winning our latest award: Large Technology Supplier of the Year. This really was a stunning achievement secured against some of the biggest and most prestigious competitors we could face. Well done everyone!

Do not underestimate internal fraud

In part one of this article we revealed the typical profile of an internal fraudster, examined the drivers of internal fraud and looked at strategies to manage the problem. In this issue we look specifically at fraud within the customer services and procurement departments.

Fraud within Customer Services

Fraud within customer services is a growing problem. One of the explanations for this is that organisations are increasingly holding their customer data in one place, making them vulnerable to internal abuse.

Another reason is that the growth in call centres has led to changes in the type of staff employed: they are generally young and inexperienced, relatively poorly paid and there is a high turnover rate, often leading to temporary agency staff. Crucially, they tend to be limited in their loyalty.

Your customer service employees are the most susceptible to an approach by organised crime gangs

Organised criminals specifically target staff in these types of positions with a view to gaining customer information and data that they can profit from. The organised criminal will:

- Identify staff open to corruption
- Identify high value accounts for takeover
- Identify dormant accounts
- Obtain information on security processes and policies
- Compromise data by passing it to other criminals
- Change details on accounts
- Transfer funds
- Obtain security answers required for authentication/verification

Examples of Customer Services Fraud

Customer service employees are ideally placed to manipulate internal systems to the benefit of friends, relatives and/or external fraudsters. Examples include:

- Removal of suspension or barring - using the billing system
- Carrying out manual recharges on prepaid subscribers
- Assigning credit to postpaid subscribers
- Illegally billing charges to other accounts - usually medium to large corporate customer accounts, which increases the time taken to detect the fraud and usually only comes to light following customer complaints
- Activation of accounts without the proper documentation
- Reactivation of accounts that have previously been closed down
- Abuse of loyalty programs, for example applying promotional credits to friends and family accounts

Identifying and Managing Customer Services Fraud

There are a number of options fundamental to the success of identifying and managing customer service fraud. Regular audits are vital, for example: reconciliations between the network and billing system; looking for customers with abnormal behaviour or severe bad debt after removals; and comparing line requests for service with line activations provisioned.

Exception reports will assist in identifying repeat restoration of services following suspension or barring, or application of incorrect tariff or charging rate plans.

Make full use of your CRM audit logs by switching them on! It's important to be able to retain a historical record of all changes made by all users for subsequent analysis. Investigate access (or attempted access) to sensitive or classified information for any suspicious cases. Furthermore, regularly monitor those employees with access levels that allow insertions or changes to billing information.

Reviewing the work environment will also help to prevent fraud. Initiate a clear desk policy and ban the use of personal mobiles or PDAs in the office (provide lockers for personal belongings). Create a paperless environment or provide shredding for confidential waste. Restrict access to email/Internet facilities and disable all ports for external devices, along with the print screen function.

Finally, don't forget to use your fraud management system. It can be very useful in detecting internal fraud, saving hours of manual work.

Using rules to monitor:

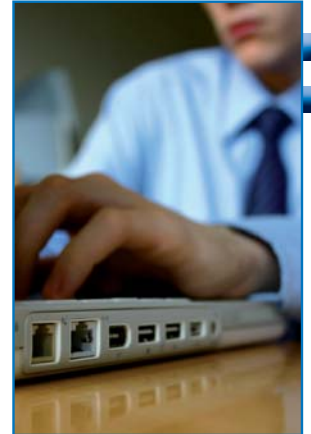
- 'Same name' matches, e.g. account holder has same/similar name as staff member accessing the account
- Patterns in combinations of data, e.g. balance transfers made and recent change of address or customer detail changes
- Aggregation of events, e.g. the number of credits/manual recharges by volume, frequency and amount per agent

Scorecard analysis, for example:

- Transaction pattern analysis
- Behavioural pattern analysis

Using profiling to:

- Create a customer call fingerprint. This allows new lines to be profiled and compared against the account profile



Procurement Fraud

Typically procurement fraud involves an employee working with an outside vendor to defraud his employer. This can take several forms: bogus or inflated invoices, services and products that are not delivered, work that is never done, contract manipulation or employee kickbacks (when an employee processes inflated invoices from a vendor and in return receives a percentage of the invoice price as a kickback), creation of fictitious suppliers, theft of physical assets, intentional overbilling by suppliers, pay and return of goods and supply of inferior or incorrect products.

Carefully examine documents for:

- Excessive credits or account write-offs
- Altered documents
- Duplicate payments
- Unusual document sequences
- Unusual or familiar handwriting
- Photocopies used as source documents
- Missing documents

“If you do not look, you do not see, conversely, once you know what to look for and go looking for it, you are more likely to find it.”

Price Waterhouse Cooper

Additional red flag indicators are:

- False invoicing - once dummy suppliers are added to the master file
- Invoices for consulting - harder to audit or check service was delivered
- Submitted invoices that have not been folded - which means they have been created in the office
- Addresses with PO Box numbers
- Contact number is a mobile number
- Sequential numbering of invoices
- Invoice total a 'round' number (sum)
- Favourable payment terms
- Sequential purchase orders for same supplier – a common tactic is to split orders to ensure they don't breach the authorisation limit

Preventing Procurement Fraud

The first step is to create an approved supplier list. Verify each vendor to make sure the company exists and that the address is valid (having a website does not mean there is a company, nor does an answering machine).

Establish a due diligence process for all acquisition and procurement matters, e.g. comparing the number of contracts issued to a list of qualified suppliers to determine whether there is an even distribution. As part of the approval process for sub contractors or agents include a questionnaire on suppliers' business practices, and require them to sign a pledge adhering to an ethical code of conduct, guidelines and external audit rights.

Statistics will tell you most procurement frauds are discovered as a result of a tip-off or audit, however there are a number of preventative measures you can take. For example, carry out regular checks to see if any employees hold directorships in

any supplier companies. Also monitor supplier details, such as name, address, bank account numbers etc., and match them against employee records (seek advice here from your legal department). Furthermore, periodically carry out physical checks, counts and reconciliations to the general ledger.

“Recent studies suggest that over 60% of data breaches originate from an internal source or event.”
Ponemon Institute

Finally - Create Staff Awareness of Fraud

Creating staff awareness of fraud, and creating a code of conduct for staff with access to sensitive information, is proven to greatly reduce the problem. Anti-fraud training shows employees how to identify the early signs of fraud and provides them with strong and direct messages of support should they ever need to report fraud. There are huge benefits to be gained from fostering an anti-fraud internal culture, which defines clear processes and policies, and communicating this clearly to all staff. There should also be a reporting mechanism, such as a whistleblowers' policy and/or a hotline, to facilitate the reporting of suspicious behaviour.

The aim of staff anti-fraud training should be to create an environment in which employees believe that dishonest acts will be detected, are not to be tolerated and will be punished.

Hayley Daniels is a member of the Institute of Counter Fraud Specialists and former Fraud Operations Manager with Hutchison 3G UK. She chaired the Training Group at TUFF (Telecommunications UK Fraud Forum) for five years and has served on the TUFF Board of Directors.



At Neural Technologies Hayley provides fraud management consultancy and training, including hosting the company's programme of educational online seminars.

Fixed Line Revenue Opportunities

According to a joint study by Arthur D Little and Exane BNP Paribas, European fixed-line operators are in a strong position to ride out the recession due to the opportunities presented by 'triple play' services, i.e. the bundling of home phone, broadband access and television delivered over the Internet.

Key findings include:

- The ongoing success of Triple-Play helps operators to limit fixed line losses, maintain average revenue per user (ARPU) and preserve profitability through market consolidation.
- Halving the rate of fixed line losses over the 2008-15 period could increase an incumbent operator's valuation by 27%. Some European operators have already shown that this is possible.
- Fixed European operators will have a €4BN revenue opportunity by 2015 from content and services related to the 'TV of the future'.

To download the report, entitled 'Reviving the Fixed Line', visit www.adl.com.

Company News

New! Fraud and RA Workshops

Neural Technologies has hosted two fraud and revenue assurance workshops in Malaysia in response to calls from several Asian Pacific telecommunication operators, who wanted more in-depth, hands-on knowledge than that provided by the commercially-run revenue management conferences in the region.

Topics for the interactive workshops comprised internal and procurement fraud, COSO framework and best practice techniques in problem solving and analysis. Attending operators included Time DotCom, DiGi, Maxis, U Mobile, MobileOne, StarHub and Telekom Malaysia.



Hayley Daniels hosts Fraud and RA Workshop

Said Sonny Gomez of Maxis, "We found Neural Technologies' workshop to be extremely beneficial. Completely unbiased, it provided us with a wealth of knowledge and valuable insights into revenue management techniques, which we will be putting into practice on our return. Furthermore, it provided us with an ideal opportunity to network and share information with our peers".

Adrian Keet, regional Director of Business Solutions in Asia Pacific said, "The positive feedback and overwhelming success of the workshops shows there is a crucial gap in the market for such comprehensive, hands-on training. Due to the popularity of these initial workshops, we will be making this a regular occurrence in Asia Pacific and rolling out a series of workshops in Latin America, the US and Europe".

Any operators interested in attending these workshops should contact louise.penson@neuralt.com.

Beat the Recession with our Revenue Sharing Model

Neural Technologies is enabling telecoms operators to beat the global recession by offering its risk management software solutions on a pay on performance basis. What this means is that if its solutions do not deliver the expected results, organisations do not have to pay!

Luke Taylor, Neural Technologies' Commercial Director explains, "In these uncertain times operators need cast-iron guarantees that any solution they implement will deliver the promised results. This revenue sharing option gives operators the confidence that everything possible will be done to ensure the success of their project".

The pay on performance scheme requires no licence fee for the software, just nominal implementation and training fees. Operators agree mutually acceptable and pre-defined targets with Neural Technologies, and thereafter only pay when the solution satisfies those targets. For further information contact ntl@neuralt.com.

Trilogy USA and Orange Poland Go Live

Neural Technologies has completed the installation of its Minotaur™ Fraud Management Solution for Trilogy International Partners, providing protection for two of Trilogy's subsidiary mobile operators - Voila in Haiti and Viva in the Dominican Republic. Future subsidiaries will be added, and plans are in place to extend the solution's capability to tackle other revenue management issues.

Carol Wilson, Trilogy's Project Director of Operations, said, "The hosted Minotaur™ solution enables us to rapidly bring new subsidiaries on line and protect our revenue from the outset. Furthermore, the solution gives us more in-house control over configuration than our previous system. This enables us to respond rapidly to changing market conditions, without reliance on a vendor or even our own IT department".

Over in Europe Orange Poland is also celebrating the 'go live' of Minotaur™. Pawel Surmak, Division Manager of Corporate Fraud & Revenue Assurance for Telekomunikacja Polska said, "We selected Minotaur™ over the competition based upon its superior performance, throughput capability and stable environment. Moreover, its flexible configuration, which enables us to not only keep pace with emerging fraud patterns, but also to accommodate changes to our business, such as the introduction of new products and services".

Online Seminar: Detecting and Managing Dealer Fraud

Thurs 21 May - 1000 or 1600 hours UK time

This seminar is offered free of charge to telecoms operators and has an educational focus, i.e. no sales pitch.

- Examining the sources of dealer fraud and its impact
- Identifying the most common types of abuse
- Developing and implementing strategies to limit dealer fraud
- Case study: How one organisation is successfully managing dealer fraud

To register contact meg.sawyer@neuralt.com.

Get Involved...

We are interested in receiving your feedback and would be delighted to cover any issues that you consider relevant, or to include any material you would like to contribute. Please contact us at ntl@neuralt.com