DIRECTED RISK RESEARCH PROBLEM STATEMENT

Risk Theme	Operational Risk	**Problem Nr.**	PS16008

Client Name	Christoph Nieuwoudt			**Client Org.**	FNB
Designation	Chief Risk Officer				
E-mail	Cnieuwoudt@fnb.co.za	**Tel (w)**		**Mobile**	087 311 8796

PROJECT TITLE: Fraud detection using generalised Markov random fields

PROJECT GOAL:

To develop a behavioural model that accurately identifies fraudulent nodes in a weighted and directed financial network, in the presence of noisy observations.

HIGH LEVEL DESCRIPTION OF PROBLEM:

Fraud risk is a major contributing factor to Operational Risk. The modelling and detection of fraud in complex networks is in its infancy, especially in South Africa

It is proposed that a model for fraud detection be developed, using connectedness between individual nodes in a complex network. A narrow interpretation of connectedness may be the number or values of transactions between individuals (network nodes). A broader interpretation may include other common features that may discriminate between fraudsters and non-fraudsters such as gender, age, rank, account activity levels and so on. The premise is that fraudsters and money launderers are connected through transactions and other features. The proposed method could use these links to improve classifier performance by factoring in the effect of such links between individuals, using a generalisation of a well-known model that was initially developed for statistical physics (the Ising model), which models the spins of atoms in a crystal lattice structure. The general form of such models are known as Markov random fields, and are also extensively used in image processing. These models could potentially be further generalised to potentially link any individual (node) to another, not only neighbouring nodes as in the case of a crystal lattice or digital image

PROJECT OBJECTIVES:

This project aims to enhance existing fraud detection methods by using connectedness between individuals. A bank typically has fraud detection systems that classify one individual at a time, thereby ignoring the links between individuals. Given some network of fraudulent and non-fraudulent nodes that further contains clusters of nodes that have above average connectedness, the algorithm can use the network connections to improve fraud classification results, which will in turn reduce the load on human analysts investigating potential fraudsters. This could greatly improve the efficiency of counter fraud efforts in banks and lead to significant savings

OUTPUTS REQUIRED:

- A paper in the academic financial literature
- Practical Guidance to the industry on local / international best practice

STRATEGIC VALUE TO DIRECTED RISK RESEARCH:

Improved accuracy of fraud detection systems will result in significantly improved operational efficiency and saving of costs. Nodes in a network that are identified as fraudulent will need to be investigated individually. Hence inefficient fraud detection models that yield large numbers of false

positives lead to excess costs for the user. Moreover, inefficient models are more likely to miss fraudulent nodes altogether. In this this research, a model could be developed that improves demonstrably on current approaches to fraud detection in terms of efficiency, the more so if it could incorporate behavioural factors, which is typically absent in more traditional models