

Case Study

SiD in Banking Fraud

Abstract

Major trading banks via the banking association, had concerns in the area of types of fraud being perpetuated by individuals in multiple banks. No real data sharing capability was available to enable transfer of information. It was clear that collective information could extend the preventative and investigative power of individual banks. It was also important to appreciate the identities used in the fraud and the networks co-ordinating organised fraudulent activity.

It was also clear that the volume of transaction based fraud data available was difficult to analyse by traditional linear methods. Some form of network visual analysis was required.

A joint exercise was commissioned by the bankers' association fraud committee to provide some metrics and analysis of the information already held by individual fraud units.

Fraud data was supplied by two major trading banks. Using the generic data import capability of SiD the data was loaded to a form suitable for common analysis. Using the i2 Analyst Notebook interface – a major co-ordinated fraud ring was identified – operating across both banks. Neither bank was aware of the commonality of this data nor the complete picture of the ring and the aliases being used.



For further information

Email: info@superstructuregroup.com
Website: www.superstructuregroup.com

Head Office

Superstructure Group Limited
Ash House, Fairfield Avenue
Staines, Middlesex TW18 4AB
United Kingdom
Ph +44 870 803 2579
Fax +44 1784 224 245

Regional Office

Superstructure Group (AP) Limited
Level 1, 19 Tory Street
P O Box 19127, Courtenay Place
Wellington, New Zealand
Ph +64 4 385 0001
Fax +64 4 381 3934

Copyright © 2005 Superstructure Group Limited

All rights reserved

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Superstructure Group Limited, the copyright holder.

This document is the property of Superstructure Group Limited and may not be disclosed to any third party or copied without consent.

Table of Contents

Abstract	1
The Issues	1
Information Volume	1
Information Collection.....	1
Internal Fraud	1
Security.....	2
Identity Matching	2
The Approach.....	2
An integrated Investigation and Intelligence Capability	2
The Solution.....	3
SiD.....	3
Security.....	3
Identity Matching	3
Analysis	3
The Results.....	3
Case Study	4
First Cut Result.....	4
Rapid isolation of Areas of Interest	5
The Payback: SiD Value	6

The Issues

Information Volume

The data available to fraud units is often extracted from large corporate transaction record systems. The volume of such information is large and it is exceedingly difficult to glean clear insights buried in the mass of information. The result was information overload on the investigators concerned – with a major problem in finding focus points to start analysis.

Information Collection

The channel for information collection in large fraud cases is automated extraction from corporate transactional databases. Typically this data will be very succinct in terms of data content and will need to be extended during the course of the investigation to provide entity-association information, linking of alias names and other details relating to the alleged fraud.

Bank systems typically have pattern/anomaly detection systems which will identify a set of potentially suspicious transactions. Many use AI or Risk Analysis techniques. Systems include:

- iHex from Oxford Universities computing laboratories;
- MonITARS (Monitoring Insider Trading and Regulatory Surveillance), developed by Searchspace;
- Visa Intelligent Scoring of Risk (VISOR); TRIAD™ adaptive control system,
- FICO® scores,
- Falcon™ Fraud Manager,
- Diamond™ mortgage origination solution,
- Capstone® Decision Manager; to name a few.

The output from such systems provides an indication of suspicious activity – but in many cases that is where the real work begins.

Internal Fraud

One of the key facts of fraud is that the majority is perpetuated by insiders. As an illustration:

The statistics on internal fraud are startling. For some organizations it is estimated that the cost of internal fraud can be as high as 6% of turnover:

- Internal fraud and abuse cost US businesses \$600 billion in 2001.
 - In Europe, the figure for 2002 promises to be even bigger than the €2.16 billion reportedly lost to internal fraud in 2000 (Association of Certified Fraud Examiners, 2001).
 - Sixty percent of all fraud involves the employees of an organization, often working in collusion with outsiders (PwC Economic Crime Survey 2001).
-

Continued on next page

Security

In many cases allegations may be sensitive because the fraud is internal. In this case the data needs to be protected with confidence – until the allegation is proved or the information is transferred to a law enforcement agency. In this case SiD military strength data security ensures absolute protection even from internal access.

Identity Matching

Fraud depends largely on the validation of false identity at one or more points in the application process. Multiple aliases and variations on identity will be used in various circumstances – with often only a few common clues to real identity. Language variations and spellings of names can cause mismatches to occur in many systems.

The Approach

An integrated Investigation and Intelligence Capability

Managing such massive information volumes requires an automated approach from outset. Information obtained from transactional systems must be extended to provide other investigative data. Such data must include relationships including critical associations with internal employees (given the high rate of internal fraud).

Clear views of the structure of organised networks conducting fraud with a particular modus can provide key information to strengthening procedures and closing loop holes. Management of the documentation must provide security, categorisation, text analysis and a logical filing structure to provide comprehensive intelligence to support future focus – but also to manage specific investigations.

The Solution

SiD SiD fraud investigation system has provided the levels of information management and investigation support for such major fraud cases for over 10 years. The document capacity is unlimited and coupled with the power of *The Mole* text content analysis – the document search and retrieval capability is unparalleled.

Security SiD's military intelligence heritage ensure the level of security is auditable to Secret level – and has proven to provide data security for the most sensitive internal investigations (which can safely operate in parallel with day to day investigations – without any fear of the unique SiD data silo protection being broken).

Identity Matching Using the SiD Identity Systems® search engine – identities can be matched against other identified fraudulent identities. The power of the Identity Systems search engine is that it operates on true fuzzy logic which can be optimised both for the language and the nature of the data being collected. The search can be extended to include key factors of identity data such as address, person gender, post code or birth date.

Within SiD the duplicate checking includes the above capability plus a probabilistic weighting on whether a person may be the same. For example if a person's driver's licence matches a licence already on file – then that person has a high probability of being the same. On the other hand a surname and one first name (“John Smith”) may have a much lower probability – but this will be increased by adding their date of birth.

Analysis SiD provided the ability to track the commodity flow of highly complex transaction and commodity flows. The intelligence analysis power of SiD coupled with the visual analysis capability of the world standard i2 Analyst Notebook® product provides detailed event correlation and commodity flow discovery.

The Results

The net result of this exercise was a clear indication of the possibility of reducing loss through extended fraud investigation capability. There were immediate benefits apparent in enabling rapid investigation focus - cutting through high volumes of data – providing a far better utilisation of investigative effort versus return. Also highlighted was the value in sharing data in a secure manner to consolidate the view from multiple fraud data sources.

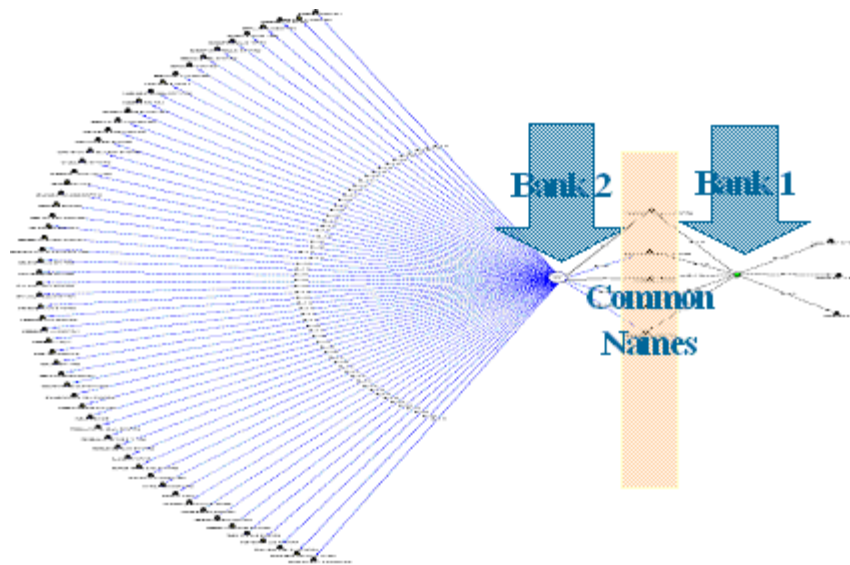
Case Study

First Cut Result

The first cut result:

- Quickly identifies common names of interest
- Highlights the need for tools to make sense of the volume of data (even at this initial level)
- Highlights clusters of interlinked activity (people and organisations involved in fraud)

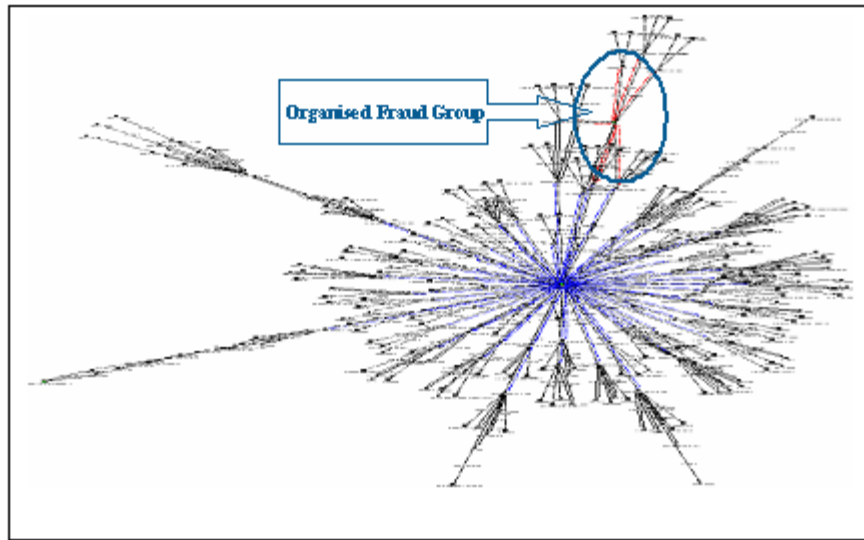
Initial Analysis



**Rapid
isolation of
Areas of
Interest**

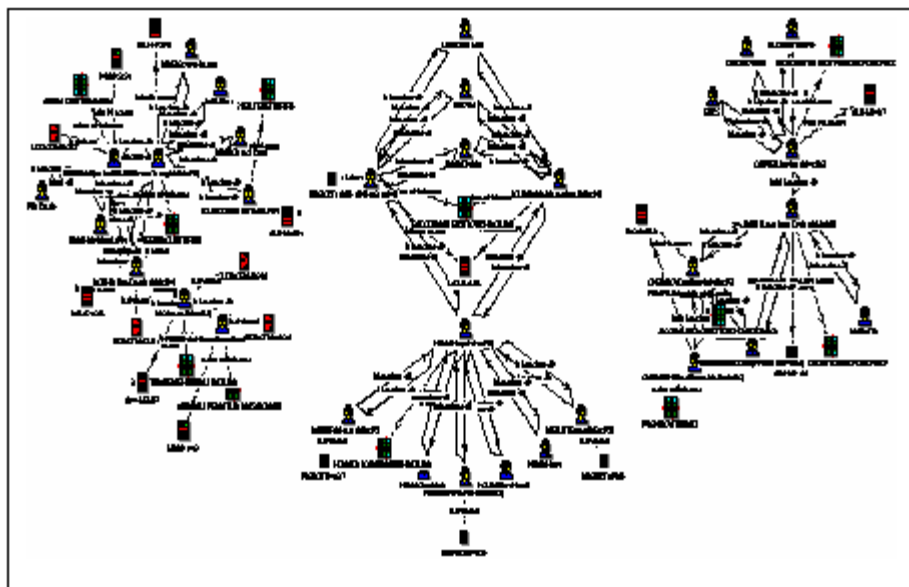
Information volume very rapidly exceeds the level where meaningful analysis can be made with tools such as Excel Spreadsheets.

i2® Analysis of Bank 1 and Bank 2 Data below – quickly illustrates areas of potential suspicious activity.



Clustering Patterns

i2 Analysis Quickly shows clusters of activity around certain Individuals or Organizations. These provide a focus for cost-effective investigation – resources are focused on key areas of interest.



**The Payback:
SiD Value**

The key payback was in the ability to provide an investigation focus point from the mass of transactional data supplied. An organized criminal syndicate was immediately identified. This focus has immediate benefit in allowing focus for the investigative team for the best possible knock-out value and eventual loss saving.

The other immediate benefit was in the recognition of the network of identities involved – some of which were known to one bank but not the other. By providing a complete network picture – the ability to enhance proactive response and greater loss prevention was further highlighted.

Each investigation gathers details of fraud perpetrators, their modus operandii and details of their identities. In large organizations – isolation of potential fraud data for analysis will allow a picture of fraud trends and minimize repeat attacks.

In a protected environment SiD can provide sharing and checking of known fraudulent identities – again minimizing the risk of repeat attacks.

SiD provides the ability to monitor and isolate activity of interest so that investigation is targeted for maximum knock-out return with the most focused (therefore most cost effective) effort.
