Internal Fraud – The Threat from Within
## Contents

Introduction ........................................................................................................................................................................................1  
Definition and context......................................................................................................................................................................1  
How does it impact the bank? ........................................................................................................................................................2  
The challenge .....................................................................................................................................................................................2  
A solution to the problem ...............................................................................................................................................................2  
Automated detection .......................................................................................................................................................................3  
The data ................................................................................................................................................................................................................3  
Join the dots ....................................................................................................................................................................................................3  
Identify the risks ...................................................................................................................................................................................................4  
Exploration and insight ....................................................................................................................................................................4  
Governance and privacy ..................................................................................................................................................................5  
The benefits ........................................................................................................................................................................................5  
Wider uses ..........................................................................................................................................................................................5  
Closing remarks ................................................................................................................................................................................ 5
Introduction

Fraud is an ever growing problem for our financial institutions, with criminals using a wide variety of methods to attack organisations across systems, channels, processes and products. Unfortunately, the role of the employee has become an area of increased focus for fraud; with employees acting both in isolation as lone individuals, but also becoming a new tool in the organised criminal’s armoury.

This paper examines the threat of internal fraud and how cutting edge technology and analytics can help institutions combat this growing problem.

Definition and context

The problem of internal fraud is one of the most wide reaching fraud typologies, spanning many departments, roles, processes and systems. As a result, it presents a financial institution with a very real challenge of ‘where to begin’.

Rather than examining internal fraud as a single problem, it is best viewed as the employee acting as an enabler for a wide range of fraud types. The diagram below presents just some of the typologies currently faced:

- **Theft from Customers**: The most understood and prolific internal fraud type is the theft of a customer’s money. Typical modus operandi include siphoning funds from vulnerable customers’ accounts, often elderly customers and dormant accounts, or taking over a customer’s identity in order to submit new lending applications.

- **Credit Abuse**: The employee utilises their position and knowledge of the bank to authorise credit either for themselves or for those they know. The intention is not to defraud the bank of money, rather it is an abuse of their position to give unauthorised credit and hence, puts the bank at additional risk.

- **Breaches of Policy**: At their most minor, breaches of policies amount to little more than a managerial reprimand, e.g. an employee has been browsing on the accounts of their favourite footballer. However, these have often been seen to be precursors to more damaging behaviour. This could include recognising that as an employee you can search/browse on famous people’s accounts and leak the information to the press, or make transactions on the accounts of your friends and family.

- **Money Laundering**: An employee knowingly opens an account and processes transactions for customers to launder their money. This can often involve multiple employees working in collusions who circulate and submit fake KYC information.

- **Procurement Fraud**: Employees facilitating fraud in connection with vendor and suppliers of the institution. This can include conflicts of interest (undeclared relationships with suppliers/vendors), invoicing and transaction fraud, financial kick-backs or even non-existent ‘ghost vendors’.

- **Trading Fraud**: This includes the well-published unauthorised trading cases such as Jerome Kerviel at Société Générale, along with market abuse activity such as Libor/rate rigging and market manipulation. This can be a challenging area for the bank where controls are typically weak (simple rules based) and often sit in silos within the bank.

- **Expenses and Payroll**: Financial organisations are beginning to examine and monitor their expenses and payroll processes in more detail. This is an area where the losses are unknown and where data is poorly captured.

- **Data Theft**: Protecting the bank’s data from theft is high on the agenda for data security and cyber crime teams, with the focus on protecting systems from external phishing and malware attacks, as well as ensuring employees are unable to remove personal information.
The reasons why an individual may commit this type of fraud against their employer have been studied at length, with identified triggers including external pressures (both financial and personal), unhappiness at the treatment by their employers, greed – the list can be long. Interestingly, the most high profile cases of internal fraud have been committed by long term employees who understand best how the bank operates and who might previously have been considered the most loyal.

Ultimately, inadequate and ineffective internal controls allow this activity to take place, whilst poor warning systems prevent early detection. Therefore banks must take a two-fold approach to tackling the problem – improving governance and process as well as implementing accurate, flexible and sophisticated detection systems.

How does it impact the bank?

The impact of such events can be devastating, not least the financial implications. By way of example one only has to examine some of the recent high profile cases to hit the news, such as those at Société Générale (a €4.9 billion trading fraud)\(^1\), RBC ($1.1 million theft)\(^2\) and Lloyds (£2.4 million invoice fraud)\(^3\).

As well as the huge financial losses, the damage to the reputation of the bank can be significant. Bank employees are trusted and respected individuals – and any suggestion that they may act in a fraudulent manner calls in to question the relationship that individuals will have with that organisation. Put simply, customers will lose faith in their bank if its staff cannot be trusted to safeguard their finances.

The challenge

For many organisations, there are no systems and processes in place to safe-guard their business from this type of fraud. Even for those that do have systems in place, incidents in recent times show that the traditional approaches being taken are no longer adequate in the fight against internal fraud – they are unable to identify the warning signs of activity early enough and if they do trigger alerts, they do so with high false positive rates.

There are a wide range of reasons for this:

- Organisations are siloed by line of business – they don’t/won’t can’t share their data, this includes across the multi-channels now available

- Traditional systems act on events in isolation, e.g. a transaction or an application, meaning that it cannot piece together the complex events and relationships that are normally associated with internal fraud cases

- Detection techniques used are simple; rules, whilst they inject business expertise, can easily be determined and therefore offer limited protection in isolation

- Inefficient and ineffective investigation tools – internal fraud is a ‘sensitive’ issue and an investigation must be efficient and accurate to ensure that the right decision is made.

These organisations must begin to look at the next generation of solution available. The remainder of this paper explores this approach.

A solution to the problem

Technology has made major advances in recent times, particularly with regards the ability to analyse large volumes of data very quickly. The challenge of detecting internal fraud is, at its heart, a ‘big data’ problem. With the development of high performance analytics and in-memory processing, fraud detection systems can and must look past traditional rules-based approaches and use the data they have available to its full potential.

Advanced technology enables banks to implement a bi-lateral defence strategy. It will always be necessary to look for the patterns you know you want to look for, but it is also necessary to be able to identify these in a more accurate and automated fashion.

1 http://en.wikipedia.org/wiki/J%C3%A9r%C3%B4me_Kerviel
3 http://www.bbc.co.uk/news/uk-england-london-19675834
At the same time, one must be able to search for the “needle in the haystack”, enabling users to visualise, explore and understand their data at the touch of a button, without dependency on IT departments and within a reasonable response timeframe.

Manifestations of internal fraud that are normally tackled as a single business problem are those of ‘theft, credit abuse and breaches of policy’. This paper will use these business problems as an example to examine this approach in more detail.

Automated detection

The roles generally associated with these types of internal fraud are typically those that have access to customer accounts, transactions and credit applications, e.g. that of branch staff and managers.

The data

The data trail that will allow a solution to identify the relevant modus operandi is substantial, both in terms of volume and number of sources - customer data, application data, financial and non-financial transactions, employee footprint data (e.g. account touched or looked at), known fraud and bad debt customers/accounts etc. This data may well be held in different places, in different formats and often with varying levels of data quality and thus requires the use of dedicated data management, manipulation and integration tools.

Join the dots

Once ingested, solutions must be able to draw new intelligence out of the data. Whilst volume was previously seen as a blocker to the identification of high risk activity, when used in the correct way, it is the facilitator.

Using both direct and indirect (fuzzy) matching techniques (such as phonetic matching, spelling distance and pattern patching), high performance solutions can overcome both poor data quality and intentional manipulation of data, to create a single view of all the entities that exist within the data, from employees, to companies to individuals, to addresses etc.

Furthermore techniques such as social network analysis (SNA) can automatically link and build networks across the bank’s internal data, as well as data provided by third parties, to create a complete networked intelligence picture. This effectively creates a single view of an employee’s activities across all the transactions they have made, accounts they have touched, applications they have processed, and buildings/systems they have accessed as well as their registered addresses, telephone numbers and other contact information.

The networked intelligence picture is used in two key ways. Firstly, risk assessment; applying detection methods across the social network levels is proven to significantly increase the amount of fraud detected, the speed at which the fraud is detected and the quality of the fraud detected (reduced false positive rates etc.). This will be explored in further detail in the following section.

Secondly, the visualisation of social networks is extremely effective in aiding a more efficient investigation. Our solutions offer this visualisation as part of the management of an alert, and includes full drill down to the underlying data needed for investigation.

Figure 3: Process to produce a networked intelligence warehouse

A complete intelligence picture of combined data for customers and the employees who interact with them.
Identify the risks

The networked intelligence picture is the foundation upon which accurate risk assessment and earlier detection of risk can be achieved.

Using the output of social network analysis technology, a solution can risk assess across three levels:

1. **The event** – an application for credit, a transaction on an account, a log record within a system.
2. **The entity** – an employee, a person, a company, an address, a telephone number etc.
3. **The network** – the relationships that exist between entities.

Across these three levels, a hybrid approach to risk detection can be applied that facilitates the identification of both known and unknown fraud scenarios. The hybrid approach includes the following techniques:

- **Business Rules**: Business rules are the simplest form of detection, but should not be overlooked. They are a way of encapsulating the knowledge of your most effective fraud investigators, by encoding their knowledge across three levels: what makes a particular event (e.g. a transaction) potentially risky, why an entity (e.g. employee, address) is risky and what the associated risks of a network connected to that entity are. For example, ‘an employee logs in to a high wealth account, changes the address, reissues a credit card and this is followed by a high value cash withdrawal’, or ‘an employee has processed a credit card application for someone socially connected to them.’

- **Anomaly Detection**: A particularly powerful technique to identify fraud not previously seen or to risk score one entity or network against its peer group. Example techniques include: K-means cluster analysis or Kohonen Vector Quantization. In the context of internal fraud, examples may be ‘unusually high volume of browsing on vulnerable customers’ accounts, e.g. high wealth, dormant, elderly, etc.’ or ‘the employee is acting on accounts outside of his normal geographic area.’

- **Advanced Analytics**: The analytical techniques available to organisations is extensive, including advanced modelling algorithms; decision trees, gradient boosting, bootstrap forest, least angular regression splines, neural networks, linear and logistic regression, partial least squares regression, survival analysis, time series data mining, incremental response/net lift models and many more.

- **Text Mining**: Text mining is becoming an increasingly powerful capability with the rise in use of blogger sites such as Twitter and Facebook. Best of breed solutions offer a wide range of text mining capabilities which are used in isolation for unstructured text analysis, as well as in combination with structured text to provide an enhanced view of the entity/network of interest for risk assessment. At a high level, text capabilities include:
  - Text Parsing: Part-of-speech, noun group and multiword term identification
  - Text Filtering: Term stemming, misspelling identification and synonym detection
  - Topics of interest:
    - term and frequency weighting and filtering out irrelevant terms
    - Common concepts throughout emails
    - Clusters terms into groups
    - Identify key topics and phrases e.g. terms related to trade confirmations
  - Automatic entity extraction based on part-of-speech tagging and pattern recognition
  - Identify interrelationships between categories, concepts and entities
  - Automatic fact and event discovery:
    - Find out who was doing what (and when)
  - Sentiment analysis:
    - Extract expressions of views within free text
  - Build dynamic ontologies across document repositories:
    - Use advanced linguistic analysis to establish hierarchical relationships of semantic terms
  - **Database Searches**: Providing the ability to automatically check an entity or the details of an application or transaction against the intelligence repository. This may contain known fraudulent applications or transactions that were alerted as being fraudulent. It may also contain third party adverse data or hotlists.

This approach ensures that returning threats are not accepted into the bank even if they use different combinations of details about themselves to avoid being identified.

The result of utilising this combination of techniques across the layers of the social network is an automatically generated aggregated risk score of an event, entity or network of entities for early warning signs including internal fraud, credit abuse or misconduct such as compliance breaches.

Exploration and insight

To complement this automated approach, financial institutions are looking for new ways to explore their data – to quickly and easily drill down through the data to explore areas of risk not previously considered. Using in-memory processing and
user-friendly data visualisation, best-of-breed technologies can give users the power to ask questions on the fly. Millions of rows of data can be analysed in seconds, without reliance on IT, with the results presented in a user-friendly and highly visual way.

This, in turn, provides a continuous feedback loop to the detection model, enabling risks discovered during the exploration stage to be fed back into the on-going detection models. This final point is critical – staying ahead of the curve is a must for banks. In order to achieve this, any system that is implemented must be flexible and able to evolve as and when the bank, and indeed the criminals, do.

Governance and privacy
The governance model surrounding an internal fraud solution is of critical importance.

There is a need to have tighter and more consistently monitored controls – after all, prevention is better than cure. This may mean enforced segregation of duties, better controls and restricted access rights, as well as providing improved visibility to management.

However, it will not always be possible to prevent internal fraud. It is not an issue that will generate hundreds of alerts per day; however, when suspected cases are detected, it is a specialist team that must lead the investigation in a structured, auditable manner, with involvement from HR and legal departments. The reputational damage of incidents of internal fraud can be huge and a dedicated team committed to the prevention and detection of this activity is critical.

One other consideration is the need to monitor personal employee data and the questions this raises around data privacy. Ultimately, to accurately identify high risk activity before it is too late (either to protect reputation or financial losses), extensive data is required so that full relationships between employees and customers can be understood. However, it must be handled sensitively, with full understanding and interpretation of the laws, and the good news is that many financial institutions are now managing to bridge this gap, being able to both detect the activity of high risk employees, whilst safeguarding the privacy of their good employees.

The benefits
Reputation, and the protection of it, is central to the benefits financial institutions can realise from a best-of-breed internal fraud solution. Through the more accurate identification of high risk employees, banks can protect their customers and their systems and processes from this internal threat.

Accurate detection facilitates earlier identification of fraudulent activity and indeed the identification of new frauds that may not have previously been discovered, thus reducing the financial exposure to the operational risk and fraud committed by employees.

The operational impact of these high performance solutions should not be under-estimated. Accurate identification of fraudulent activities means an improved false positive rate (investigation of fewer incorrect cases). Furthermore, the visualisation of data described above enables investigators to be more efficient as they work cases.

An interesting by-product of implementing a sophisticated internal fraud solution is the ‘deterrent effect.’ Whilst difficult to measure or quantify, it is known that employees will be considerably less willing to commit this type of fraud if they are aware that unusual activity is being closely monitored.

Wider uses
One point to note is that the usage of this networked picture does not have to be limited to just the detection of internal fraud. The internal fraud network picture is the foundation in the identification of 1st party fraud (i.e. customers who get credit with the intention not to pay it back), both at the point of application (Application Fraud), as well as during the customer lifecycle (Bust-Out/Sleeper Fraud). There are also the more positive use cases, sometimes referred to as the ‘white side’, where for example, the marketing team may want to identify relationships between the banks’ customers in order to exploit opportunities of positioning new services or products.

Closing remarks
The manifestation of fraudulent activity committed by employees can unfortunately affect every corner of the bank. Financial institutions must strengthen their processes and systems in order to prevent fraudulent activity where possible. Where prevention fails, these institutions must then use best-of-breed technologies to assist in more accurate detection and earlier warning, before the bank feels the true impact of these fraudulent activities.

Data and analytics is at the heart of this – if used in the right way, high performance solutions running on vast quantities of data can unlock a huge amount of business value for every organisation.