

Waste, error and fraud – applying innovation to reduce public sector costs

The downturn in the Irish economy and focus on cost reduction in the public finances has undoubtedly increased the focus on the elimination of waste and error, as well as the detection and prevention of fraud. A recent Ernst & Young study found that half of Irish organisations surveyed have suffered, what they consider to be, serious fraud in the last two years. This compares to just 16% of organisations globally and 21% in Western Europe. Of particular note from this research is that, as organisations focus on reducing costs and improving processes in the downturn, many are uncovering pre-existing fraud schemes which went largely undetected during the boom years.

Parallels can be drawn with the public sector, where similar analysis is ongoing to reduce the cost associated with waste and fraud. However, the breadth and volume of services delivered by the public sector present challenges for managing the risks of fraud, waste and error. The public sector is the largest employer in the State, providing services and entitle-

ments to the general public, through multiple systems, across multiple departments, procuring goods/services from thousands of suppliers along the way. Such complexity naturally leads to challenges when it comes to managing waste, error and fraud.

by accident'. However, such methods are limited in their effectiveness and only scrape the surface, particularly when organisations, such as the public sector, maintain vast quantities of data.

While there have been some positive advances in recent years in terms of fraud detection and waste elimination, these traditional methods are no longer sufficient on their own and more effective and innovative fraud and waste detection strategies are now required.

One key area which is becoming critically important in this respect is how any organisation use the data it collects to detect anomalies, and in doing so proactively prevent fraud, waste and error.

Examples of where this could be applied in the public sector include:

- Detecting benefit fraud where person is receiving welfare payments even though they do not meet eligibility criteria (e.g. based on income)
- Identifying overpayments to suppliers by analysing historic procurement data
- Identifying errors and anomalies in payroll such as excessive overtime payments

The Irish Government has recognised the potential in this area and the recent Programme for Government and committed to a major

anti-fraud enforcement drive supported by the "latest available technology and better sharing of data across government departments and agencies".

While the successful deployment of these techniques to combat welfare fraud offers the greatest potential for cost savings, it is also possible to use the same approach to identify waste, error and fraud in



Eoin O'Reilly.

catators of fraud, waste and error and investigate further – e.g. flagging social welfare payments being transferred under multiple names but into the one bank account etc.

A further complication in the public sector is that public services are managed by several departments and there is no single data repository which can be used for proactive analytics. Even within individual departments there are often several systems used to deliver services and this presents challenges in providing comprehensive and consistent sources of information. While it is generally accepted that there needs to be an increased level of data sharing between Departments and State agencies, there are legal and data protection implications to consider around the level of information that can be shared and how such data must be protected.

However, these challenges can be overcome – several countries for example, have introduced codes of practise for public authorities sharing data for the prevention of fraud.

Detection versus review

An important distinction in the deployment of data driven fraud detection techniques is the distinction between fraud detection and fraud review.

- Detection is the process of identifying and prioritising potential fraud, waste and error from available data within an organisation
- Review involves the

confirmation that fraud has actually taken place and includes the process of taking corrective actions when it has, such as blocking payments, recouping paid monies and prosecution.

In recent years, many organisations have focused on fraud review, improving their review procedures through internal audit and 'special investigations'. However, the challenging task of detection – i.e. effectively identifying suspects in the first place – has received less attention although this clearly offers the greatest opportunity for significant return on investment if addressed in a comprehensive fashion.

Mining for gold

The starting point in identifying waste, fraud and abuse is the analysis of historical data that you already have in your systems.

Detection is a statistical game with the goal of improving the odds of finding the target. The process is analogous to fishing for rare fish in the ocean. Without the right tools, you are left to fish the endless sea of legitimate activity for your rare fraudulent catch.

Not surprisingly, a tremendous amount of time and effort can be spent to identify a single suspect case. A good detection system will filter the entire ocean and help identify a small pond where the odds are much more in our favour.

Fishing in a well stocked pond translates into substantial savings because the system to focus expensive human effort and expertise on reviewing those activity records that are most likely to pay off.

The effectiveness of a detection system can be quantified using the following two measurements:

- Detection rate - the percentage of total fraud isolated in the pool of suspects -and
- False positives rate - the ratio of legitimate to fraudulent entities in the pool of suspects.

Experience has shown us that, with the deployment of an effective detection based fraud monitoring system, the detection rate goes up, the false positives go down and a more effective result is achieved in terms of time, cost and recovery.

These sophisticated detection systems combine data matching algorithms with a statistical model-based approach which allows an organisation to more effectively and accurately detect fraud by highlighting situations where fraud is statistically most likely to occur. The models 'learn' from the data associated with real instances of fraud and look for similar patterns in the wider population of data – for example, in the public sector, this principle can be applied for means test data, benefit payments and procurement entries.

Data linking and matching

The key to the performance of any detection approach is the ability to automatically carry out fraud detection over a large number of different data sources such as person records, entitlement assessments, payments and life events. Fraudsters work hard to disguise their true identity and details in order to appear "normal" each time they repeat their fraudulent behaviour.

Their techniques have evolved to evade current simple matching systems which aim to detect identical pieces of data e.g. names, addresses, telephone numbers etc. However, these simple matching systems cannot always correctly link records where there might be minor differences in, for example, the spelling of someone's name or address, or the format of their telephone numbers.

In the example below, the table below would not be matched using simple data matching as the format of the dates of birth and telephone numbers are slightly different.

However, in recent years more sophisticated data matching have been developed to overcome these hurdles and also enhance the linkages between records.

One might still want to link or associate two records that do not match directly together if they are indirectly matched via a third piece of data. In the example, there is no immediate link between Record A and Record C when looking at name, date of birth or telephone number. However, there is overlap between Records A and B (surname and address) and overlap between Records B and C (date of birth and phone number). As a result there is direct and indirect connection between all three records and so this may warrant further detection. A simple matching technique however, would not identify this (Fig. A).

Conclusion

While positive progress has been made in recent years reducing fraud and error, the Government has made it clear that the level of waste, error and fraud in the system remains unacceptable. A fresh approach is needed to deliver the cost saving targeted and to combat the increased sophistication of fraud schemes.

The use of advanced data analysis has proven highly effective in fraud detection in the retail banking, credit card, property and casualty insurance and health-care insurance industries, where they typically can reduce fraud losses by up to 20-50%. These techniques are now also being used to track down benefit and occupational fraud, error and waste with remarkable results. The results of detection efforts can ultimately feed into fraud prevention programmes to prevent future occurrences of the same type of fraud.

By Eoin O'Reilly – Advisory Senior Manager – Ernst & Young

Fig. A

Record	Name	Date of Birth	Telephone No.	Address
A	Sean Murphy		01 7654321	Apt 3, 80 Long Road, Bigtown, Dublin 6
B	John Murphy	16.01.1958	+353 86 555 5555	3/80 Long Road, Bigtowne, Dublin
C	E. Ryan	16/01/1958	0865555555	65 Short Street, Dublin 2