Deloitte.

Deloitte Review

Caught in the middle

How government contractors and other businesses can use analytics and continuous monitoring to address improper payment risk across the value chain

Improper payments by government and its agencies and departments happen for a variety of reasons, including inadvertent errors, inadequate controls and, in some cases, wilful acts of fraud.

Whatever their cause, improper payments – that is, overpayments, duplicate payments, underpayments, payments made without substantiation, or payments otherwise involving fraud, waste, abuse or errors – are in the government's crosshairs as never before.

The growing call from the public and politicians to identify, report and mitigate or at least minimise the effects of waste, fraud and corruption, abuse and errors is reflected in stricter laws and regulations and sustained public outcry against such indiscretions.

Most business leaders, especially prime contractors to government, and civil servants recognise that these expectations to proactively deal with the scourge of fraud and corruption, along with the clamour for greater accountability, will likely lead to an increase in investigations with the purpose of recovering irregular payments. However, these stakeholders may not understand the extent to which, and by what means, they need to add depth and rigour to **detect, respond** and **prevent** fraudulent activity. Rather than relying primarily on whistle-blowers and tips to unearth problems, it has become imperative for government and business alike to start using sophisticated analytics to identify and investigate irregular payments that have already been made. Some government institutions and businesses are beginning to use predictive analytics and near-real-time transaction monitoring tools to catch errors before payments are made.

These changes have implications for both prime suppliers/contractors and subcontractors/suppliers. Prime contractors/suppliers are generally subject to greater scrutiny and accountability, including investigation into their use of subcontractors/suppliers. The prime contractors/suppliers are responsible for irregular payments made to their subs, even if they are not aware of, or involved in, the irregular or fraudulent action/payment.

How can companies lessen the risk of becoming a national news story due to irregular payments caused by misdeeds of a subcontractor or its own employees? Also, from an internal operational efficiency perspective, how can they curb their own losses attributable to fraudulent payments?

The answer lies in adopting robust strategies, processes and tools to proactively root out waste, fraud, abuse and errors. Advanced tools wielded by analysts experienced in antifraud programmes can assist organisations and government alike – to identify and recoup irregular payments.

Such initiatives are neither simple nor cheap, and some senior executives may balk at making such a commitment solely for compliance or even risk management purposes. However, along with addressing regulatory requirements, government and business can use these new approaches and technologies to achieve other business objectives, such as identifying and resolving areas of spend/revenue leakage across their respective value chains and refining operations across the enterprise, including strategic planning, operations, marketing and human resources.

Past, present and future – a look at analytics and monitoring tools

The arsenal available to governments, contractors and other businesses to identify irregular and otherwise inappropriate payments consists of three broad categories of activity:

- **Data analytics and forensic analytics tools** – Used forensically to look at historical payments already made in search of anomalies indicative of potential improper payments
- **Continuous monitoring tools** – For reviewing, in real time, disbursement activity in search of anomalies that might indicate potential irregular payments
- **Predictive analytics tools** – Used to identify actions, behaviours and trends (based on statistical probability) that might indicate the likelihood of future irregular payments

To address the increasing risks associated with irregular payments, government and other businesses should implement high-tech analytical and monitoring programmes that are focused on payments made and received. A clearer understanding of the tools involved – and the types of expertise needed to use them effectively – can help government and businesses to decide which might be most helpful in their respective environments.

Data analytics and forensic analytics – looking into the past to detect

Generally speaking, forensics involves combing through data on past activities, events and transactions to identify issues and anomalies. Forensic analytics is superior to traditional auditing techniques, because it is capable of testing virtually 100% of a population instead of sampling only a percentage. The process includes anomaly detection tests (or rule sets) that are run against normalised data sets and analysis of the results by forensic accountants, also known as forensic auditors. The number, type and complexity of anomaly detection tests depend on the type of irregular payments being targeted. Examples of anomaly detection tests that can be employed include, but are not limited to, the following:

- Duplicate payments
- Payments to debarred or suspended government contractors
- Payments to fictitious addresses
- Payments made outside normal working days, i.e. during holidays and weekends
- Round number payments, especially once-off such payments
- Multiple payments relating to the same requisitions, order numbers or invoices
- Payments to different bank accounts in respect of same supplier

Continuous transaction monitoring – looking into the present to prevent in the current and into the future

The best defence in mitigating losses from improper payments is simply preventing such disbursements from being paid out in the first place. A strategy built around prevention is many times more effective than one founded on “pay and chase”, i.e. investigate later, even if that “pay and chase” strategy is powered by the advanced analytics capabilities described above.

Continuous monitoring is a relatively nascent technology that provides access to this type of protection. The technology equips businesses and government with the ability to detect, respond and prevent irregular or other inappropriate payments in real time. This technology works by screening each transaction against a predefined list of characteristics or “rules” and by making automated decisions about that transaction based on the result of this real-time analysis. Depending on the needs of the organisation, a transaction can be automatically denied or passed along to other workstream functions for additional review. This type of technology is just beginning to penetrate both business and government.

Predictive analytics – looking into the future to identify

Predictive analytics is a methodology that utilises machine learning and statistics to analyse historical and current data to predict future actions and events, i.e. using hindsight to develop solutions with insight and to implement these with foresight.

Using advanced analytics and algorithms, such as econometric models, neural networks, decision trees and self-organising maps, data can be mined for trends, patterns and behaviour that will provide, for example, indicators of anomalous activity that go beyond rule-based detection. In short, one variable, or a number of variables acting in concert, are analysed to assess whether a relationship exists with other variables of interest.

Potential benefits of predictive analytics include:

- Accelerated identification of anomalous activity early in the process
- Reduced false positives and increased accuracy regarding suspected behaviours
- The ability to incorporate updated information and findings to continually refine the predictive model
- The ability to identify new schemes or patterns without prior knowledge

Application of predictive analytics is varied. Studies might involve views into fraud detection, price optimisation, product demand forecasting, customer segmentation and loyalty, or the effects of geospatial distribution.

Managed Forensic Framework – combining the past, the present and the future

It is possible to combine the best attributes of data analytics, continuous monitoring and predictive analytics into an even more effective approach. Essentially, the elements of past, present and future can be viewed and analysed in one hybrid fraud detection framework. This affords an organisation even deeper insight into the nature of its payments and the effectiveness of its operations.

In this type of multi-dimensional technology platform, incoming payment data is streamed down two parallel paths – one that operates in a "live" environment and the other in an "offline" setting. At a high level, the continuous monitoring technology is deployed in a real-time or live stage, with predictive analytics and forensic data analytics being completed in an offline stage.

As discussed previously, the transaction data streamed in the live environment is screened with rules and runtime models to make real-time decisions – for example, a pay or no-pay review. With the hybrid approach, the results of these dispositions are sent to the offline analytic setting for further assessment.

There, it is possible to query the data to make the monitoring process more effective. Was flagging a particular transaction effective? Should the rules be modified or optimised? If the rules or models are changed, how many more or fewer transactions will be flagged? Are there emerging trends? Clearly, these are the types of questions that are appropriate for an offline platform – and predictive analytics in particular – rather than slowing down the monitoring function that is applied to live data.

The benefit of this architecture is that, in effect, it acts as a giant feedback loop. This is important because perpetrators of fraud continually modify their approach as they learn about new thresholds, whether imposed by governments through new laws or by companies that are simply more vigilant. Companies should continually evolve and refine their capabilities to keep pace with potential fraudsters.

However, the benefit extends beyond fraud. Are the same types of payment processing errors or waste occurring? Can error patterns be identified by frequency or source? If so, this type of insight can guide an organisation about how and where processes can be enhanced.

Lastly, given that this hybrid approach captures and analyses historical data in the offline setting, an organisation can incrementally add a forensic querying interface that allows data to be viewed through a different lens. With the mechanism for collecting and storing payment data already in place via the monitoring functionality, this additional capability can be included efficiently. In fact, it is entirely possible that insight gained through this forensic interface can be used to further inform the rules and models used to screen live payment data. This effectively gives the organisation aspects of all analytic worlds in one package.

Prerequisites for establishing analytics and monitoring capabilities

Businesses and government can and should leverage the power of analytics and monitoring tools. These tools provide insight on transactions that can be used by organisations to mitigate and help with the recovery of irregular and other otherwise erroneous payments, as well as to provide value to strategy planning and operational areas across the enterprise.

Specifically, in an era where transparency and accountability are emphasised increasingly, analytics and monitoring tools help government to:

- Mitigate some of the risks associated with responding to government inquiries and investigations
- Protect and enhance their corporate image
- Recoup potential inaccurate payments
- Save taxpayer and shareholder funds by deterring fraud and mitigating escalation of possible fraud, waste or errors

Benefits derived from advanced analytics and monitoring tools do not end with compliance and recovery. Businesses can gain traction with other diverse and critical business imperatives, including:

- Addressing uncertainties in formulating business strategy
- Assessing business workflow to improve quality control, logistics and distribution
- Analysing customer behaviour to refine customer relationship management and market segmentation
- Providing business intelligence in support of workforce planning, recruitment and talent management

To capitalise on these advancements, some companies may need to elevate certain aspects of their existing organisation, approach and capabilities.

Contacts

Dave Kennedy
Leader, RA Forensic, Southern Africa
Managing Director, Risk Advisory, Africa

Direct: +27 (0)11 806 5340
Mobile: +27(0)82 780 9812
Email: dkennedy@deloitte.co.za

Tommy Prins
Director, Risk Advisory, Forensic

Mobile: +27 (0)82 824 2815
Email: tprins@deloitte.co.za

Navin Sing
Director, Risk Advisory, Forensic

Direct: +27 (0)31 560 7307
Mobile: +27(0)83 304 4225
Email: navising@deloitte.co.za

Clayton Thomopoulos
Director, Risk Advisory, Forensic

Direct: +27 (0) 21 427 5680
Mobile: +27 (0)82 749 4638
Email: cthomopoulos@deloitte.co.za

Gregory Rammego
Director, Risk Advisory, Forensic

Direct: +27 (0)11 806 5255
Mobile: +27 (0)82 417 5889
Email: grammego@deloitte.co.za

Marc Anley
Director, Risk Advisory, Forensic

Mobile: +27 (0)79 893 8191
Email: maanley@deloitte.co.za

Praveck Geeanpersadh
Director, Risk Advisory, Forensic

Direct: +27 (0)11 806 5437
Mobile: +27 (0)82 450 7387
Email: pgeeanpersadh@deloitte.co.za

Graham Dawes
RA Leader – Rest of Africa

Mobile: +254 719 892 209
Email: grdawes@deloitte.co.ke