

South African Payroll Association

10 October 2019

Fighting Payroll Fraud with Technology

Authored by; Rob Bothma, Exco member of the South African Payroll Association (SAPA)

Last month I spent some time speaking at the various South African Payroll Association's regional annual conferences, focusing on fraud in payroll. In my preparation for these talks I decided that I would focus my talk around the impact emerging technologies are currently having with regards to compliance in the payroll department.

During my research on this topic one of the scariest things I found was that, although on the one hand technology can be used to assist the HR and Payroll teams in fighting fraud, it was also being used to assist employees in committing fraud.

One of the scariest facts coming out while gathering information for this talk was the amount of fraud being committed with regards to "*ghost employees*", in both the private and public sectors.

When looking at what technologies are available to fight this and other acts of fraud within payroll, the newest and probably the most powerful is no doubt the use of Artificial Intelligence (AI), which includes various technologies such as:

Machine Learning, which provides the ability for systems to learn and improve from experience without being explicitly programmed to do so. This process starts with analysing large amounts of historical data, to provide the input required to create the relevant algorithms, which once created can then be utilised against the organisation's current data to start providing predictive analysis results.

Analytics, which can be utilised for the creation of real-time dashboarding, presenting data in an easy to view visual representation, which can be extremely informative, in standard pie and bar charts format, which are easy for users to interpret.

Blockchain, which utilises distributed ledger technology, which is essentially a system of record where many copies of a record are stored across various servers, ensuring that no one individual can edit a record without the "*approval*" of all other parties. Think of an individual's education record, which is essentially co-owned by all parties but cannot be manipulated by the individual themselves, thus providing a record that can be trusted by all parties who have access to it.

Another area which I raised in these talks was the whole issue of **Audit Trails**. Being involved with software vendors for the past 30 odd years, I never ever came across an organisation that did not specify that any payroll solution they would use, needed to have full audit trail facilities which at a minimum would record details such as before and after

images after every transaction, who initiated the transaction as well as the usual date and time stamping.

Two challenges:

1. Did any of the payroll managers present actually know which staff members had administrator access to the Audit Function?

By having the capability to switch auditing off and on, creates an ideal environment for fraud. In the past I have come across organisations where this loophole was successfully used by a payroll staff member who unknowingly to management, had the system authority to turn auditing off, where they were able to reinstate a resigned employee, change the banking details to their own, and then run a payroll payment through the system before switching auditing back on again.

2. When last did anybody in the organisation actually analyse any of the payroll audit trail data?

My research found that the average time it takes to identify fraud in payroll was 18 months, as reported by the Chartered Institute of Payroll Professionals, which in itself a scary thought. But when understanding that the bulk of payroll administrator never bother to look at payroll audit trails, it's easy to understand why it takes so long.

The detail of much of the payroll fraud being conducted today actually resided in the audit trails, the organisation really just needs automated and intelligent tools to be able to analyse this data and alert the relevant staff members when anomalies are encountered.

And this is where Analytics can play a big role. Have real time data being displayed, can help with not only detecting fraud but also empowering management to take immediate steps in stopping fraudulent transactions before they can be completely processed.

With the power of emerging technologies having the ability to "*learn*", this makes them extremely powerful when it comes to analysing data, providing both analytical results and predictive indicators, empowering HR and management with true decision support capabilities.

By taking this learning capability and applying it to fraud prevention, it is easy to see how new-age systems are able to create patterns of behaviour based on historical data, and then quickly being able to identify when a change in pattern or an anomaly is encountered.

For example, a payroll user who suddenly starts editing employees' bank account details or starts creating new employee records in numbers that are way above the norm. It's not to say that these are not valid transactions, but by being alerted by a change in behaviour empowers the organisation's risk team to investigate the relevant transactional detail, enabling them to assess the situation to determine the probability of fraud being committed.

One of the downsides of using sophisticated technology is that sometimes areas of risk can be hidden within the configuration of the system, and as such, can often be overlooked, and in this example, who has been assigned the administrator rights to controlling the Auditing function.

Another big contribution to fraud is the lack of visibility regarding segregation of duties.

It is very difficult to manually monitor each and every user's access rights on a continual basis, as new users are continuously being added and while other being deleted, making this a cumbersome task that eventually gets ignored. This is the ideal breeding ground for the *ghost employee* phenomenon.

If an unauthorised user can create a *ghost employee* and then have the ability to execute a payroll run for them, this is a fraudster's paradise. No wonder my research uncovered so many examples where millions of Rand were being lost through payments made to non-existent *ghost employees*! In each of the cases, there was either no control on the segregation of duties or collaboration between staff members to overcome this control.

In summary, the tools to both fight and prevent fraud in payroll have become extremely sophisticated and are now available to organisations of any size.

Payroll managers need to take an urgent look at the limitations of their current systems and ensure that these are mitigated through either replacing the current payroll solution or at the very least ensuring that the payroll is upgraded to a version where these AI capabilities are available, to ensure that fraud in your payroll is eliminated in its entirety.

MEDIA CONTACT: Rosa-Mari, 060 995 6277, rosa-mari@thatpoint.co.za,
www.atthatpoint.co.za

For more information on SAPA please visit:

Website: <http://www.sapayroll.co.za/>

Twitter: [@SAPayroll](https://twitter.com/SAPayroll)

LinkedIn: [The South African Payroll Association](https://www.linkedin.com/company/the-south-african-payroll-association/)