



*We care about your business*

# Theron Le Roux

## Accountants / Rekenmeesters

Assosiaat Algemene Rekenmeester (SA) • Associate General Accountant (SA)  
Professionele Rekenmeester (SA) • Professional Accountant (SA)  
Belastingpraktisyn • Tax practitioner

38 Akasia Street George East 6529 • 4529 George East 6539 • Tel: 044 871 5067 • Fax: 044 871 5082

**WITH COMPLIMENTS**

e-mail : [jgmt@jgmt.co.za](mailto:jgmt@jgmt.co.za)



[Forward email](#)

[Online Printable Version](#)

KEEPING YOU IN TOUCH

ca[sa] .news



**In this Issue**

**Beware of Cyber Crime – It's**

**November 2013**

## Growing Rapidly and You Are At Risk!

- *What is cyber crime and how prevalent is it?*
- *Why target small businesses?*
- *What can we do about it?*

## Tax Tips 2013

- *What you should do*

## Check for CV Fraud: The Costs Can Keep Mounting

- *What to do if an employee has faked his/her credentials*

## Finance 101: What Exactly Is “Quantitative Easing (QE)”? And Does The End Of QE Mean Trouble For Our Economy?

- *What is QE? Oiling America's economy – how it helped us*
- *Where does that leave South Africa? The pincer threat in the wings*
- *What can we do about it?*

## Your Tax Deadlines For November

 **Subscribe**

## BEWARE OF CYBER CRIME – IT’S GROWING RAPIDLY AND YOU ARE AT RISK!



*“The infectiousness of crime is like that of the plague” (Napoleon Bonaparte)*

Isn't it terrible how many dangers are lurking out there? One of them is cyber crime and small businesses (with less than 250 staff) are increasingly being targeted.

**South Africa is particularly vulnerable as we are naive when it comes to protecting our assets, know-how and trade secrets.**

### What is cyber crime and how prevalent is it?

It is using technology (Internet, computers, software and smartphones) to steal data, property, IDs, passwords or money. It also includes the destruction of data or software via viruses. Phishing, corporate espionage, and stealing from your bank account are examples.

Cyber crime is illegal in South Africa and offenders contravening ECTA (the Electronic Communications and Transactions Act) are liable to up to five years imprisonment.

It is difficult to get actual facts as crime statistics do not separately isolate cyber crime. Experts are also convinced it is widely under-reported. A recent survey done in South Africa showed only 7% of businesses said their systems to prevent data leakage were working well. Police statistics show that white collar crime has risen 56% since 2006. South African banks reported that phishing increased by 61% in 2011.

England, not surprisingly as a first world economy, has more experience with cyber crime. In 2011, GBP27 billion was lost to cyber crime, of which GBP21 billion (almost 80%) is attributable to small businesses.

For an eye-opening look at the staggering levels of cybercrime globally (did you know for example that over 600,000 Facebook accounts are compromised daily?) see the Infographic at <http://www.go-gulf.com/blog/cyber-crime/>.

### Why target small businesses?

Small businesses do not have the resources to actively combat cyber crime and thus are easier targets for perpetrators of cyber crime. They are vulnerable to phishing and bank fraud but, more significantly, they are also exposed to theft of intellectual property (IP) and industrial espionage.

**In the above UK research, of the GBP21 billion losses attributable to small business, most of the cyber crime came from theft of IP and corporate espionage.**

There is no doubt this is more prevalent locally. Apart from there being widespread ignorance, security experts are scarce and much of our IT security is outsourced to foreign companies. We have recently seen how the United States is eavesdropping around the globe and we need to ask just how secure are we? How much of our intellectual property and trade secrets end up in overseas companies and countries?

### What can we do about it?

As a starting point, we should review our controls and security. Staff should be aware of phishing and similar practices and should be warned to be careful about what information they share on social media sites. Systems should be put in place to monitor and respond to such incidents.

In terms of losing our IP and being vulnerable to espionage, this requires substantial resources and needs the involvement of government security agencies. The

Electronic Communications and Transactions Act of 2002 provided for the appointment of “cyber inspectors” with police-like powers to monitor for, and investigate, cyber crime, yet this is still to happen. A grassroots advocacy campaign from business to get this cyber crime force off the ground is a significant option to look at, and the recent appointment by government of a “National Cyber Security Advisory Council (NCAC)” is a positive step in this regard.

### TAX TIPS 2013



Tax season is upon us with eFiling income tax returns due for non-provisional taxpayers on 22 November 2013 and provisional taxpayers by 31 January 2014.

Recently, SARS has codified penalties for things such as late submissions or understatements of income. More information flows to SARS from third parties about income you have earned – just look at how your tax return is already populated

by retirement funding and your IRP5 information, for example.

**As SARS are under pressure to maximise collections, you can expect more queries on your tax return. In view of the additional information SARS has and the potential penalties you could pay, it is necessary to approach your return in a new light.**

#### *What you should do*

1. Plan your return. Familiarise yourself with the transactions which flowed through your bank statements. Make sure you know what you can claim and what is disallowed. Seek advice from your accountant / tax practitioner to clarify any uncertainties you may have.
2. Have a filing system and document all tax deductions. Remember you are required to keep your documentation for five years. It pays to be disciplined upfront. Doing a tax return is bad enough but don't compound it by trying to find documents when doing the return. You will probably miss potential tax deductions by not organising your documentation. Remember SARS are likely to ask for documentation.

When you download your tax return, it will already be populated with information from your IRP5, interest and dividends received, and retirement contributions or retirement income received. All of the relevant institutions will have sent you copies of the data submitted to SARS - check that this is the same as the information on your tax return. Any differences should be sorted out with the relevant institution prior to submitting your return.

You will also need:

- A log-book if you receive a car allowance or enjoyed the right of use of an employer-provided vehicle.
  - A section 18A certificate if you made a donation to a Public Benefit Organisation (PBO). You are allowed to claim up to 10% of your taxable income for donations made to approved PBOs.
  - Invoices or other relevant documentation in respect of any other claims you intend making. For example, if you run a business to earn a second income, expenses attributable to that income can be claimed if you have the necessary documentation.
  - All documents of any out-of-pocket medical expenses you incurred (see 3 below).
3. This is the first year of the medical rebate. Previously tax deductions were allowed. These reduced your taxable income. Rebates reduce the tax you pay.

In addition, you are entitled to deduct out-of-pocket medical expenses subject to criteria laid down. It is worth seeking professional advice to ensure you maximise the deduction allowed.

4. If you make use of a tax practitioner, check he/she is correctly registered with SARS.

#### **CHECK FOR CV FRAUD: THE COSTS CAN KEEP MOUNTING**



Since the global financial crisis, jobs have become harder to find. This is not just a South African phenomenon but is happening worldwide. It is no surprise that as jobs get scarcer, so job hunters push the boundaries when submitting their CVs.

In South Africa, CV fraud is becoming more frequent. Employing the wrong candidate is costly in terms of time and money wasted and it can go further than this – imagine employing a quality control “expert” in a food manufacturing facility and reading in the paper that consumers got seriously ill digesting your products!

It applies to all job strata – in 2012 the CEO of Yahoo reportedly lied about his qualification. It has reached the stage where the University of South Africa (UNISA) has prosecuted 94 people who submitted fake qualifications to get entry into the university. Recently two people were caught in possession of 1,000 UNISA certificates.

#### ***What to do if an employee has faked his/her credentials***

Labour law will have to run its course. You will need to give the staff member adequate notice of a hearing and allow the employee to put his/her side of the story. The verdict of the hearing will depend on the facts of the case. For example, the case of a staff member who lied about an adverse credit history may result in a different outcome if that person has access to cash or is for example a sales representative.

The costs and time involved in employing someone with a fabricated CV can just keep mounting.

Investing time in getting the right person is worth it. There are reputable accreditation agencies out there that can check qualifications, credit and criminal history. Put thought into the interview process. Set prospective staff members a skills test, e.g. if they are going to join your public relations department ask them to “prepare” a press release if a certain scenario occurs. Spend time checking references and it very often pays to have more than one person involved in the interview process.

Research in the USA shows that two thirds of new staff members leave within a year of employment if no proper selection process is used. Apart from the time and cost involved, your business could suffer real losses.

#### **FINANCE 101: WHAT EXACTLY IS “QUANTITATIVE EASING (QE)”? AND DOES THE END OF QE MEAN TROUBLE FOR OUR ECONOMY?**



We follow the news and the outlook for the economy seems to be increasingly negative. The words “Quantitative Easing (QE)”, “balance of payments”, “the Rand falling” and “strikes” are often bandied about.

**Where does South Africa stand economically? It is important to all of us as the economy has a fundamental impact on business – and on our savings.**

### ***What is QE? Oiling America's economy – how it helped us***

When the global financial crisis hit markets in 2008, the US Federal Reserve Governor, Bernanke, was particularly worried about the collapse in liquidity. When money stops circulating, activity in the economy drastically reduces and without working capital many businesses cease trading. The economy goes into a downward spiral.

The problem facing Bernanke was interest rates were too low to effectively use as a monetary policy tool. So he committed the Federal Reserve to buy medium to longer term commercial assets. The purchase of these assets injected money into the banks. Substantial assets were (and continue to be) purchased and this "oiled" the economy as massive amounts of liquidity stimulated the US and global economies.

This oversupply of dollars started circulating globally to find the best return. At that time, the best performing economies were emerging markets and they became the beneficiaries of this liquidity. **South Africa, as an emerging economy, experienced massive off-shore purchases of its bonds and shares.** This supported our currency as it covered our trade deficit. It also stimulated economic activity as is evidenced by the record index on the Johannesburg Stock Exchange..

### ***Where does that leave South Africa? The pincer threat in the wings***

The first problem is that QE is clearly a short-term strategy – once the US economy resumes normal growth and unemployment drops to below 7%, then QE will be "tapered off" until it stops. For the past year, there has been increasing speculation that the Federal Reserve will "taper off" its asset purchases.

This has led to worries about the Rand and it has dropped by 30%. The weakness due to worries over QE has been exacerbated by our trade deficit continuing to widen. For the first eight months of the year it has come to R107 billion or 6.5% of gross domestic product. It is 54% up on last year.

Thus, we face a potential pincer threat to our economy – the easing of QE will reduce the appetite of foreigners to finance the trade deficit combined with the ongoing deterioration in our trade deficit. The impact of this may lead to further Rand deterioration, rising inflation and a reduction in economic growth.

### ***What can we do about it?***

There are two things we can do -

1. Raise interest rates – this will support the Rand but will reduce growth in the economy
2. Grow exports to reduce the trade deficit. Exports to Africa are rapidly expanding which is partially off-setting weaknesses in the Euro zone (this is our largest export market). Ending industrial action will also spur export growth.

### **YOUR TAX DEADLINES FOR NOVEMBER**

As noted above, non-provisional eFiling taxpayers must submit their income tax return by 22 November.

### ***Have a Great November!***

Note: Copyright in this publication and its contents vests in DotNews - see copyright notice below.

© DotNews, 2005-2014 CA(SA)DotNews is a division of DotNews, proprietor Stanhope Trustees SA (Pty) Ltd, Reg. No. 1999/017337/07.  
Web site: <http://www.dotnews.co.za>

Copyright notice: no part of this newsletter may be used, redistributed, copied, imitated or reproduced without prior written permission of the owner.

#### **Disclaimer**

**"CA(SA)DotNews" is a general information sheet and should not be used or relied on as professional advice. No liability can be accepted for any errors or omissions nor for any loss or damage arising from reliance upon any information herein. Always contact your financial adviser for specific and detailed advice.**