BAKER TILLY
MORRISON MURRAY
Auditors, Accountants & Business Advisers

Accounting Matters

Vol. 2 Issue 3
November 2012

BEWARE: BIG BROTHER SARS IS WATCHING!

Taxpayers beware: SARS are now going to third parties to collect information about you. They already have all your IRP 5 information captured on their system – you can easily see this if you are on E-filing.

SARS have now written to all banks and financial institutions requiring them to send a return to SARS twice a year, containing the following:

- Account number, identity number or registration number of the owner, whether the account is FICA'ed, and income tax number of the account holder
- Amounts deposited, invested or lent to the taxpayer
- Interest received or accrued to the taxpayer
- Monthly movements on the account i.e. totals of debits and credits on the account
- The first return covers the period 1 March to 31 August 2012 and the second from 1 September to end February 2013.

What does this mean? To date institutions have sent IT3s to taxpayers detailing the amount of interest earned or paid and the final balance on the account at the end of February. It's possible (although not clear) that SARS will have this information loaded directly on their system and when you do your 2013 return, SARS may already know how much interest you earned or paid.

Be ready for queries

The other significant point is that SARS will have access to your transactions and may ask you why, for example, there was a large deposit into your account and whether the deposit is included in your taxable income. *Be ready to answer any such queries so you don't get yourself into an awkward situation with SARS.*

Now that SARS is getting information from third parties about you, one wonders what their next step will be. Big Brother is getting closer all the time!

YOUR WILL: THINK, AND PLAN IT

We don't like to think about our mortality. At the same time we don't want to leave our affairs in a mess for our family and friends to sort out. Not giving careful thought to your estate could reduce the benefits to your beneficiaries. It could also be financially harmful to them.

The starting point: what do I own and what do I owe?

1. Write down all of your assets. To ensure you account for them all, check your records and check with your accountant and any other financial advisers you have. It is funny how sometimes assets pop out we never knew we had.
2. What are my liabilities? Most of the information should flow from your assets. *Don't forget things like sureties you may have provided* – these may be called up on your death. If so, you need to plan accordingly. You also need to be aware of what happens to your liabilities after you die. Some will be paid out with insurance policies, like mortgage bonds and others will, as with sureties, fall due for payment. We need to plan for any eventualities.

What falls into my estate for estate duty and what is excluded?

Some of your assets do not fall into your estate such as certain exempt life insurance policies (others are "deemed" to be property in the estate). These proceeds go directly to your nominated beneficiaries. The important consideration here is to keep track of all beneficiaries and make sure they are registered with your insurance company, so that paying them out runs smoothly after your death. As you can see, your will is an ongoing process and needs continuous updating – diarise to do so at least annually.

Other assets excluded altogether from your estate are pension fund and other retirement payments made due to your death. Be aware that pension fund trustees have the right to alter amounts you leave to your heirs.

The first R3.5m of your estate is exempt from estate duty, as is anything you leave to a surviving spouse (a bequest to your spouse firstly falls into your estate, but is then allowed as a deduction). As the R3.5m abatement per estate is now portable between spouses, correct estate planning could give you a potential total rebate of R7m in the estate of the second dying spouse.

These exclusions and abatements are important as estate duty of 20% will be levied on the remaining gross value of your estate. Clearly, you will want to minimise estate duty payable.

Note:

1. The assets mentioned above do not fall into your estate for estate duty purposes, but they may be taken into account when calculating executor's fees etc.
2. Estate planning is a complex exercise, and there are many potential pitfalls – you need for example to take possible Capital Gains Tax implications into account. Seek proper advice to ensure that your estate is optimally structured, and consider having your will drawn professionally.

Who do I want to leave it to?

Once we are on top of our assets and liabilities we need to decide who will be a beneficiary and how much will each one inherit? Again we need to give this careful consideration, bearing in mind the discretion pension fund trustees have.

Should I appoint an independent executor?

You need to satisfy yourself that your executor(s) has the requisite skills to administer your estate. You should also bear in mind that your heirs may fall out over the will. If you have doubts, it will be worth appointing one independent executor who will bring experience and impartiality to the winding up of your estate.

Estate planning should not happen in your old age. Start as early as you can and keep monitoring and, if necessary, updating your will.

HOW DO YOU FILE YOUR EMAILS? IT COULD BE IMPORTANT

An avalanche of information

There's no doubt that emails have become our main method of communicating in our business dealings – it is estimated that 90% of our correspondence is by email. It used to be a Herculean task to archive physical documents. The ease of email has meant that the number of documents we create has risen exponentially.

Many businesses faced with this avalanche of information delete emails after a certain period – perhaps as little as three months. Contrast that with the US where all emails are routinely kept for a period of three years.

The risks - and how to avoid them

What are the implications of not keeping emails and/or having no easy way of retrieving them?

The courts now recognise emails as a source of evidence. Laws require us to keep documentation for laid-down periods – for example SARS requires fifteen years. Thus, if we replace our emails on a regular basis, we run the risk of potentially destroying evidence. And that could even be a criminal offence – Goldman Sacks paid a US $8 million fine for destroying emails central to a criminal case. Further, if we have a dispute with a staff member it could be important to have kept a record of his or her emails to see for example if they have been defaming their colleagues or abusing their email usage.

Government has passed legislation on electronic communications, including emails. The Electronic Communications Act lays down how emails are to be stored:

- The information is to stay in its original format (this is to prevent tampering with emails)
- The origin and to whom the document was sent must be identifiable. The date and time the document was sent are also to be shown
- The emails are to be easily accessible

From this it is clear that management needs to have a good document management system along with good use of technology and robust controls like limiting access to sensitive information and good storage facilities. Firewalls, back-ups and a disclaimer policy also come into the mix.

The Constitution guarantees every citizen the right to privacy and part of a document management system must be to put stringent safeguards in place to protect private personal information.

Risk considerations and good governance also dictate that control of information, well indexed for ease of retrieval and kept safely for a minimum period of time is implemented by the business.

So how long should you keep emails?

Finally, how long should the information be kept? It depends under which Act it falls – SARS as mentioned is fifteen years. A rule of thumb (and it is only a rule of thumb, so take advice in any doubt) would be to keep all information not governed by specific legislation for three years. After three years prescription lapses so it makes sense to keep information for at least three years.

In summary, don't take this lightly - there is much to consider in how we treat and store our emails.

TAX CLEARANCE CERTIFICATES – A VICTORY FOR THE TAXPAYER

Many of us have experienced the frustration of applying for a tax clearance certificate only for SARS to inform us, for example, that there is a missing VAT return from 2001 or that the PAYE reconciliation (the EMP501) for 2006 does not balance.

The onus is on us, the taxpayer, to produce the relevant VAT return or EMP501 and prove it was submitted timeously and correctly. In the protracted negotiations that follow, we often find it is easier to double pay, say, the VAT on the missing return than to undergo the time and frustration of proving our case to SARS. Only once we have gone through this pain, are we given a tax clearance certificate by SARS.

What is a tax clearance certificate and why is it so important?

It is a certificate issued by SARS stating that all of our returns are up to date and that we have paid all of the taxes payable to SARS. It is valid for a certain period – usually six months. There is no law governing tax clearance certificates – they are governed by internal SARS policies.

Tax clearance certificates are called for in many circumstances, and are specifically needed for most offshore investments and tenders (particularly for government and local municipality tenders - without a tax clearance certificate businesses cannot be considered for the tender). Thus, for many individuals and entities, tax clearance certificates are crucial.

The High Court lays down the law

The North Gauteng High Court recently handed down a judgment which involved the revoking of a tax clearance certificate by SARS. In this case there were allegations of fraud against a Close Corporation (CC) and a member of the CC. Based on the fraud allegations, SARS withdrew the tax clearance certificate which the CC needed for a tender.

The CC argued that it had not been given the opportunity to rebut these allegations and accordingly the revoking of its tax clearance certificate was unlawful. Judge Wright of the North Gauteng High Court agreed with the CC, which "was entitled to reasonable notice of SARS' intention to call the certificate into question and an opportunity to put its case to SARS." This accords with the fundamental tenet of administrative justice that before a party is prejudiced or penalised, it has the right to state its case. SARS had unilaterally revoked the tax clearance certificate and this action was unlawful.

This should be seen as a significant victory for taxpayers who can expect that SARS will follow proper administration procedure in their future dealings with you.

LABOUR REFORM: PROPOSED CHANGES YOU NEED TO KNOW

There has been much press coverage regarding proposed changes to the Labour Relations Act ("LRA") And the Basic Conditions of Employment Act ("BCEA").

These Acts have been approved by cabinet and now need to go through Parliament and the National Council of Provinces to pass into law. COSATU have been vocal in pushing for these reforms, particularly for bringing an end to labour broking.

The earnings threshold increase (from 1 July)

Firstly, let's look at what has actually come into law. The threshold of the BCEA has been increased from R172,000 to R183,008 per annum. This means that any of your employees who earn less than R183,008 now fall under the BCEA. What does this mean?

Employees earning below R183,008 per annum are protected in terms of:

- Maximum working hours per week,
- Allowed time for meals and minimum rest intervals,
- Limits on how much overtime they are permitted to work and increased rates of pay for overtime work plus work on Sundays, and
- Shift allowances and access to transport for night work.

It is worth checking on how many of your employees now fall under the BCEA. It is also worth re-reading any contracts you have entered into with employees to ensure they don't have the above protections by virtue of the wording in their contract e.g. they may have begun working for you at R170,000 per annum and now earn, say, R185,000 per annum. This would put them outside the automatic protections of the BCEA but if their contract stipulated they fall within the BCEA, then contractually they will continue to do so.

New liabilities, new restrictions

Now let's go back to the proposed legislation. What will happen to labour broking?

The main thrust of government's intended amendments is to weaken labour brokers as opposed to COSATU's demand of banning them outright. The legislation aims to protect "vulnerable workers" and achieves this by deeming that workers earning less than R183,008 per annum (the BCEA minimum) will be considered **full time employees** if their contract runs for more than six months at a single place of work.

In terms of section 198 of the LRA, these "vulnerable workers" may institute proceedings against the labour broker or the employer or both parties for any contravention of, amongst others, a collective agreement concluded in a Bargaining Council that regulates terms and conditions of employment or a binding arbitration award that regulates terms and conditions of employment. *In effect, the employer is jointly liable with the labour broker.* There are similar provisions for "vulnerable workers" on fixed term contracts.

Throughout both sets of proposals, there is a tightening up of regulations to prevent employers circumventing the Acts by delaying or appealing against rulings of labour statutory bodies.

In terms of unions, before embarking on strikes, a ballot of members is to be held and a majority of members must vote in favour of the strike. This is mainly to reduce the disorderliness of strikes which has been increasing over the past few years.

The Minister may make sectoral determinations whereby trade unions are allowed to operate in certain sectors. The Minister may also set minimum wages and minimum wage increases in these sectors. The purpose of this is to ensure worker rights in sectors where it is difficult for unions to operate, such as farms.

Trade unions may also be allowed organisational rights in certain circumstances – these circumstances would, for example, be where there is a concentration of temporary workers employed by labour brokers.

In summary, the Bills tighten restrictions around employment and time will tell if the economy will benefit from this legislation. It is worth speaking to an expert to assess the impact on your business.

WHAT PASSWORD DO YOU USE? BEWARE, THE HACKERS ARE WATCHING

Do you use a simple password so it is easy to remember? Do you also use it for all your applications where a password is needed?

The problem with doing this is that passwords get stolen – for example, 6.4 million passwords were stolen recently from Linked-In. When hackers get this sort of windfall, they run these passwords against the most used passwords. When they get a match, they can get into all your programs that have the same password.

So, what are the 10 most used passwords? And what to do about it

1. password
2. 123456
3. 12345678
4. qwerty
5. abc123
6. monkey
7. 1234567
8. letmein
9. trustno1
10. dragon

If you use any of these, change them now!

The other risk is that hackers will use the patterns of the passwords they find to crack the next most obvious generation of passwords.

Use passwords of at least eight characters with mixed numbers and words, some capitals and some signs like # or &. This will give you a strong password which is hard to hack into. Get more tips from Microsoft at http://www.microsoft.com/security/online-privacy/passwords-create.aspx .

You can also generate a strong password at a site like Symantec's PC Tools – go to http://tinyurl.com/2o5yhj.

It is still risky to use this password for all your applications (remember passwords can be stolen), so have different passwords for different sites. If you have several passwords which you know you will not remember, then use a password manager application that will remember your different passwords and can log you on to your various sites. It is not worth the risk – it's like being mugged and having all your credit cards stolen when your password is hacked.

DIRECTORS' LIABILITIES: NO ROOM FOR DELINQUENT DIRECTORS IN THE NEW COMPANIES ACT

In previous issues, we have spoken about the increased liabilities placed on directors by the new Companies Act (the Act). The Act is a balancing piece of legislation and allows increased directors' powers compared to the 1973 Companies Act. With this increased power there comes an increase in responsibility and a consequent increase in liabilities for directors.

One of the increased liability provisions is section 162 of the Act – the "delinquency" provision. The effect of this section is that directors may be barred for life from being a director (this includes holding a senior management position with "general executive control" in the company) or for up to seven years or, in the case of a lesser offence, placed on "probation" for a period of time. The director may also face civil claims and potential criminal liability.

Section 162 states that a director may be declared delinquent, or placed on probation, if that person is a director or *was a director within 2 years* of the application to a court.

The delinquency danger, and grounds for declaration

Actions that warrant being declared delinquent include:

1. Acting as a director when disqualified by the Act or by the Close Corporations Act
2. Grossly abusing the position of a director
3. Acting in a grossly negligent manner or with intent to harm the company (this includes a subsidiary of the company)
4. Acting in a manner which shows "wilful misconduct" or a "breach of trust"
5. The Act also provides that a director may be declared delinquent if he/she (or "another person" – presumably likely to be someone known to the director) "gains an advantage" from knowledge obtained as a director rather than the company or a subsidiary benefiting from this knowledge.

Who can apply to the Court to declare a director delinquent?

A fellow director, senior employee, registered trade union or any other body representing employees may apply to the court to declare a director delinquent or on probation. In addition, if a director repeatedly ignores a compliance notice, a "state organ" may also apply under section 162.

More than ever before, you need not only to act in a prudent manner, but also to be able to show that you have exercised your mind in relation to any decision you make or participate in making.

The negative aspect of such sections of the Act is they tend to scare away non-executive directors who are very important in checking on the actions of executive directors. Unfortunately, the Act does not differentiate the liabilities of executive and non-executive director. In a country where skills are short, this is a disappointing consequence of the Act.

PENALTIES UNDER THE NEW TAX ADMINISTRATION ACT – A MOVE TOWARDS TRANSPARENCY

The new Tax Administration Act ("TAA") has been promulgated and will come into operation within (according to SARS) the next three months or so.

Clearly, this should concentrate the minds of directors. One of the areas of frustration for taxpayers has been the provision in the Income Tax Act which allowed the Commissioner to levy penalties on taxpayers of up to 200% *at his discretion*. The TAA seeks to redress this by introducing criteria for the Commissioner to levy penalties.

Of importance, is that the onus is on the Commissioner to justify penalties levied. This is a commendable effort by SARS to improve transparency in their dealings with taxpayers.

The "understatement" penalties

Let's examine one of these penalties – **the understatement penalty**.

An "understatement" means:

a. A default in rendering a return; or
b. An omission from a return; or
c. An incorrect statement in a return; or
d. If no return is required, the failure to pay the correct amount of 'tax'.

If any of these situations arise, the taxpayer pays the tax owed plus a penalty which is based on two considerations – a) the taxpayer's behaviour at the time of the default and b) how the taxpayer behaved after SARS detected the understatement.

These considerations are shown in the table below:

"Understatement Penalty Percentage Table"

	Penalty to be Levied			
Behaviour	**Standard Case**	**If obstructive or a 'repeat case'**	**Voluntary disclosure after notification of audit**	**Voluntary disclosure before notification of audit**
'Substantial understatement'	25%	50%	5%	0%
Reasonable care not taken in completing return	50%	75%	25%	0%
No reasonable grounds for 'tax position' taken	75%	100%	35%	0%
Gross negligence	100%	125%	50%	5%
Intentional tax evasion	150%	200%	75%	10%

Column 1 ("Behaviour") covers the first consideration and the remaining columns cover the second consideration. As you can see SARS are trying to apply *objective criteria* when considering the amount of penalty to levy on the taxpayer. Whilst this is commendable the only behaviour defined is "substantial understatement" (the greater of R1,000,000 or 5% of tax liability) and none of the others are defined. So the Commissioner still has widespread discretion.

If this is the beginning of a quantifiable process to determine penalties, then this is to be welcomed and, hopefully, the other criteria will be defined in time. As stated above, one positive outcome is that the onus is now on SARS to justify the penalty, whereas before it was at the Commissioner's discretion.

DO YOU E-MAIL YOUR INVOICES? MAKE SURE YOU DO IT LEGALLY!

We have seen in earlier newsletters that SARS is strictly enforcing compliance with all SARS related legislation. Businesses and individuals are being penalised if they are not complying with legal requirements. As email has become the standard method of communication, it is worth checking that if you email invoices to customers, you comply with SARS requirements.

The first significant piece of legislation is the Electronic Communications and Transactions Act (ECTA). From this legislation, SARS are looking to ensure that:

- The information is to stay in its original format (this is to prevent tampering with emails)
- The origin and to whom the document was sent must be identifiable. The date and time the document was sent are also to be shown
- The emails are easily accessible

In other words, SARS will want to confirm that stored emails are the equivalent of manually filed invoices. So, it is important you comply with ECTA if you send emailed invoices.

The second piece of legislation is the Value Added Tax Act. A number of stipulations are set out in this Act:

- The first requirement is that you must apply to a SARS branch office to invoice by electronic means i.e. by email.

- The business you invoice must confirm in writing that they will accept invoices via email, subject to the requirements laid down by SARS. This confirmation is to be retained by you, the supplier, for a period of five years after the last supply is invoiced electronically to that recipient.

- Tax invoices, debit notes and credit notes must display the mandatory information required for a valid tax invoice, debit note or credit note.

- The emailed document will constitute the tax invoice. Printed copies must bear an endorsement "computer generated copy tax invoice/debit note/credit note" (as appropriate). No other tax invoice, debit note or credit note may be issued unless marked as a copy of the original document

- Emailed documentation is to be kept by you for at least five years. As SARS can investigate any matter for fifteen years, it follows you should keep these records for this period.

Make sure you comply with these laws. It could be expensive to slip up on something as simple as this.

BAKER TILLY
MORRISON MURRAY

Registered Auditors
20 Westville Road, Westville, 3629
PO Box 1098, Westville 3630, South Africa
Docex 21 Westville
Tel: +27 31 267 5300 Fax: + 27 31 267 1838
E-mail: mail@bakertillymm.co.za
www.bakertillymm.co.za