verryn&CO

audit . tax . accounting

not just bean counters ... bean growers

With Compliments

Tel: (021) 761 5955
Fax: (021) 762 0864

Email: admin@verryn.co.za
Website: www.verryn.co.za

CA(SA) CHARTERED ACCOUNTANT SOUTH AFRICA

Forward email

KEEPING YOU IN TOUCH

CA(SA)DotNews

In this Issue

October 2023

The Risky New Trust Landscape – What Trustees Need to do Now

"The common assumption is that trusts are some kind of tax

Don't Fall Prey to the Most Common Cybercrimes!

Your Tax Deadlines for October 2023

panacea...Then, conversely, from a South African Revenue Service (SARS) perspective, trusts are viewed with a degree of suspicion and mistrust. [T]he truth lies somewhere between these positions." (Broomberg on Tax Strategy)

The legal and tax landscape in which South African trusts operate has changed substantially over the last few months, thanks to changes to the Trust Property Control Act ("**Trust Act"**) and the Financial Intelligence Centre Act ("**FICA"**) by the General Laws (Anti Money-Laundering and Combating Terrorism Financing) Amendment Act, as well as new rules and requirements from SARS.

These changes impose new duties on trustees, and apply to *all* trustees, not only independent trustees.

1. **Disclosure to Accountable Institutions you engage with, and record-keeping**

   Changes to the Trust Act impose two specific new requirements on trusts to combat money laundering and crime-financed terrorism, and failure to comply is an offence. If convicted, trustees face a fine of up to R10 million, or imprisonment for a period of up to five years, or both. These requirements became effective on 1 April 2023, leaving most trustees already non-compliant.

   The first new requirement is that a trustee must disclose to any "accountable institution" (see **here** for the full list of what comprises an accountable institution, but the definition includes banks, attorneys, estate agents, long term insurers and brokers, trust companies and the like) that he/she engages with it in his/her capacity as a trustee, and that the relevant transaction or business relationship relates to trust property. The trustee must also record the details of the accountable institution the trust is engaging with.

2. **Compiling and registering beneficial ownership**

   The second requirement imposed by the changes to the Trust Act is to establish and record the beneficial ownership information of a trust; to keep an up-to-date record of this information; and to lodge a register of the beneficial ownership information prescribed with the Master of the High Court.

   This second requirement recently doubled, as SARS issued notice that trusts will now also be required to submit beneficial ownership details when completing a trust tax return, among a number of other tax changes affecting trusts, as discussed below.

3. **Filing third-party returns – the IT3(t)**

   A further onerous obligation was imposed by SARS:

   Most trusts are now also required to file third-party returns, in the same way banks report interest income and medical aids report medical aid tax information to SARS, which it uses to, for example, pre-populate tax returns.

   While trust distributions were not previously reported to

SARS by third parties, the new requirements oblige trusts to file third-party returns to SARS to declare distributions and vesting amounts to beneficiaries.

This must be done via an IT3(t) report which contains prescribed information relating to trust distributions and their beneficiaries and requires trusts to report on demographic information of the trust, demographic information of trust persons/beneficiaries, trust financial flows, and any amounts vested in a beneficiary, including net income, capital gains and capital amounts.

The ITR3(t) must be submitted by 31 May of each year. The first submission will be for the 2024 year of assessment, with the first ITR3(t) due by 31 May 2024. This is the same as the due date for IT3(b) and IT3(c) returns for trusts, which report interest, dividends, and capital gains or losses to SARS, and will certainly present practical difficulties in meeting the deadlines.

4. **Completing more probing trust tax returns**

   With the trust filing season now open, SARS has also reminded trustees that ALL trusts are required to register for income tax purposes and that the representative taxpayer – most often the trustee/s - must submit a trust return.

   SARS also recently introduced changes to the Income Tax Return for Trusts (ITR12T) with additional questions, and more mandatory supporting documents.

   As mentioned, SARS has added a Beneficial Ownership Declaration page to the trust return to record all beneficial owners, and has indicated this information will be reconciled with the information reported to the Master's Office to identify any discrepancies.

   The changes also include additional questions to determine if any local or foreign amount(s) were vested in the trust as a beneficiary of another trust, or deemed to have accrued; and the number of trusts from where these amounts were received.

   In addition, beneficiaries and donors (where deeming provisions apply) of a trust must declare their income that was vested in a beneficiary by the trust during the year of assessment in their income tax returns.

   A range of mandatory and supporting documents must be submitted with the ITR12T. Depending on the trust type, this includes the Trust Deed and Letters of Authority, details of the 'Main' Trustee who is the registered representative to SARS; Annual Financial Statements, confirmation of banking details, and resolutions/minutes of trustee meetings that document significant decisions and actions taken by the trustees.

5. **Registering as an “accountable institution”**

   Due to amendments to FICA, trustees, trust accountants and trust administrators may - in certain instances - have to register as “accountable institutions” with the Financial Intelligence Centre (FIC). See the link and comments in paragraph 1 above for the full definition of “accountable institution” but, if in any doubt, be sure to confirm with your accountant whether you need to register as an “accountable institution” in terms of the new rules, and to obtain assistance in doing so where required.

Professional assistance strongly recommended

Given all these new laws and requirements, the complexity of the processes necessary to comply, the impossible deadlines - some of which have already passed – and the hefty penalties involved, if

you are a trustee you should urgently seek assistance from your accountant to ensure you can successfully navigate this new trust landscape.

Tips for Pacing Business Growth for Sustainability

"Growth is never by mere chance; it is the result of forces working together" – (James Cash Penney, Founder of JCPenney)

Every business decision carries profound consequences for the enduring existence of the organisation, and this is no more true than when it is applied to those decisions affecting business growth. Knowing how and when to expand, open new branches, roll out new features or engineer new products takes planning and is not something leaders should be trying to do by the seat of their pants in response to external events. A meticulously crafted business growth strategy is therefore essential to plotting sustainable growth. Here are the things you will need to consider when constructing yours.

Set clear targets

You know you want to be successful, but do you know what that success looks like? Just how much money do you want to make? What do you want the lifestyles of your employees and yourself to be like? What kind of turnover and profit would you consider to be successful? What would you like your reputation in the industry to be? If you haven't considered the destination for your journey, how will you ever plot how to get there?

Talk to customers

You probably already realise the value of getting expert advice. Speaking to accountants about your finances, or lawyers about contracting just makes sense. But perhaps you have not considered that no one knows your customer's needs quite like your customers? When choosing which customers to speak to, first look to those who are your ideal customers – those people who are getting good value from your services and who are happy with your products. By speaking to them, you will slowly uncover patterns for what you are doing right and what a successful business in your industry looks like.

The next step is to speak to those customers who are not happy with your service and find out why. This will help you to uncover the opportunities you are missing, and the things you need to fix to get yourself onto the right growth path.

Don't ask these customers what you should be doing though, as changing everything based on the impressions of a few disgruntled clients is a sure-fire way to failure. Rather ask them what the challenge was that they came to you to fix, why they came to you specifically, and then what they were feeling at each stage of their journey. Once again, it is about uncovering patterns, and by asking these sorts of questions you will quickly work out whether you did something wrong, whether your services lack potential solutions the

industry might need or whether you were simply the wrong fit all along.

Now that you know what a successful client interaction looks like, and where your business is falling short, it becomes easier to see which holes will need to be plugged and where you can comfortably expand over the coming years.

Build a road map

Now that you know where you want to be, and the things that will help you to get there, the next step is to set targets within your company to move things in that direction. With your long-term goal already established, and the information you have on hand it is now easier to start breaking that long term goal into short term targets. How many people do you need to hire this year to ensure they are trained for where you want to be five years from now? How soon should your factory be upgraded to take advantage of missed opportunities? What must marketing look like now, for your customers to all know about you five years in the future?

Of course, cash flow and profitability are all going to play a part in what can be achieved now and what will have to wait. Your accountant will be able to help you prioritise your expenses, and make sure you get the most out of your investments without risking your cash flow and the related ability to meet financial obligations.

Now is also the time to institute your company KPIs (Key Performance Indicators) and get everyone singing from the same hymn sheet. Your profit needs to grow steadily year-on-year if you want to make the big long-term target, so breaking it down into manageable bite size chunks is critical. Remember to also consistently track client satisfaction, revenue per client, client retention, and employee satisfaction. KPIs help you identify what tactics are working and which aren't, so you can make adjustments to your strategy and achieve your goals.

Plan for disruptions

Before you reach your goals there are going to be setbacks. Whether its key staff leaving, new competition entering the market or surprising new developments, these disruptions are going to slow down your growth. To make sure that the impact of these is lessened it is critical that you think about diversifying your income streams to mitigate high concentration areas or reliance on one client. You should also pinpoint succession candidates for your key positions and begin training now to ensure they are ready when the time comes for them to step into a departing employee’s shoes. Try to picture which disruptions might hit the business the hardest and start threading the solutions into your targets and growth plans to ensure that when they do arrive, you are ready.

Stick to the plan

While many believe that being scrappy, flexible and prepared to change the whole business on a dime is the best path to success, history proves that long term growth instead comes from having a properly constructed plan that takes into account all aspects, including possible future disruptions, and then sticking to it. At times you may be tempted to deviate heavily from the plan, but if you are matching KPIs and growing the business, do not give in easily. Don’t make decisions on a whim and rather apply yourself to the plan, making smaller adjustments along the way as necessary. After all, you made the plan for a reason.

Why the Four-Day Working Week Just Might Happen

"We need to do a better job of putting ourselves higher on our own 'to-do' list." (Michelle Obama, former First Lady of the United States)

The four-day work week has been in the news a lot recently with a number of significant studies and trials coming out in favour of the arrangement. While many would assume that workers are thrilled with four-day weeks, but that bosses are finding it hinders business, the results do not back this up. Repeatedly, these studies are coming out in support of the four-day work week with the benefits simply racking up. Here are the reasons why it just might work:

Employees want it

In terms of work schedules, employees are increasingly seeking flexibility, with a four-day workweek emerging as their top preference, according to a recent survey of American employees conducted by **Bankrate**. The survey revealed that a significant majority of full-time workers and job seekers, a staggering 81%, express strong support for a four-day workweek over the conventional five-day arrangement.

What's more, an impressive 89% of these respondents indicated their willingness to make sacrifices in order to enjoy a four-day workweek. Among these concessions, a noteworthy 54% are open to working longer hours, while a substantial 37% are even willing to explore career changes or transition to different industries. Additionally, a considerable 27% are open to increasing their in-person office presence or working entirely on-site.

Productivity Increases

Many assumed that a four-day work week would hamper productivity, but **a recent study** in the UK that included 61 companies and more than 3000 workers found exactly the opposite. The study, which followed the companies and their workers through a six-month test of a 32-hour, four-day week, with no loss of pay for employees was the largest of its kind, making its results extremely impactful. Perhaps more impressive though, is that after the study was over, 56 of the 61 companies that were involved decided to continue with the shorter week indefinitely, and two more said they were voluntarily extending the trial.

Among the benefits reported by companies were an increase in revenue over the same period in previous years, as well as a sharp decline in resignations. One company reported a productivity increase of 22%, a lower carbon footprint as well as an increase of 88% in job applications, and a 66% decrease in absenteeism.

The results back up those achieved by a **smaller pilot program** that covered another 30 companies and 1000 employees.

Employees are happier

As for employees, well they were almost unanimously happy. Participation in the above trial led to a significant decrease in people saying they lacked sufficient time during the week to attend to their responsibilities towards children, grandchildren, or elderly family members.

Additionally, they reported feeling reduced work stress as well as better mental health, more time for exercise, better sleep and generally less negativity. 55% reported an increased ability to work. The results also suggest that the shortened workweek could lead to better gender parity as the time men reported spending with their children increased nearly double that reported by women. So impactful were these benefits that 15% of employees said there was literally no amount of money that could make them go back to 5 day working weeks.

If your company chooses to adjust your working hours to fit in with the four-day work week, there are numerous ways to do it. Do you give extra days off to make up for the shorter week, work with Fridays or Mondays off, or allow employees to simply work fewer daily hours? The various options will come with their own unique financial considerations, and you should speak to your accountant to make sure you make the most of the new situation.

Don’t Fall Prey to the Most Common Cybercrimes!

“The bottom line is that cyber risks sit right alongside rising systemic risks, and is the biggest emerging, and constantly evolving risk facing businesses today.” (SHA Specialist Risk Review 2022)

In Africa, Interpol has identified phishing – particularly Business Email Compromise (BEC) – as well as online scams, as both the biggest current crime threats, and the crimes most likely to increase in the next three to five years.

This is Interpol’s list of the prominent cyberthreats identified in the African region:

- Business Email Compromise
- Phishing
- Cyber extortion including ransomware attacks
- Online scams
- Banking trojans and stealers

Below, find out how these cybercrimes are perpetrated and how to protect yourself, your company and your employees with tips from **SABRIC** and **CISA**.

Business Email Compromise (BEC)

For 7 consecutive years, BEC attacks have been the most financially devastating cyber threat worldwide, and continue to be the most prevalent cybercrime, says Interpol. A type of phishing attack, it causes significant financial losses and often reputational damage.

It includes cybercriminals using an organisation’s email account to send out fraudulent messages with malicious links or attachments

that install malware or steal confidential information.

Most commonly, however, BEC involves cybercriminals manipulating emails, especially payment requests containing bank account details. This is because it's common business practice to send confirmation of or changes to bank details, or invoices containing bank details, via email.

In BEC attacks, these emails are intercepted - or fraudulent emails or invoices are created - changing the account details to the cybercriminal's account. Any payments subsequently made are lost to cybercrime.

A recent High Court ruling in this regard, set a precedent applicable to all businesses, as the judge noted: "… the plaintiff's case established clearly that sending bank details by email is inherently dangerous, and so must either be avoided in favour of, for example, a secure portal or it must be accompanied by other precautionary measures like telephonic confirmation or appropriate warnings which are securely communicated."

Specific BEC preventative measures include:

- Inform clients that your company will never change banking details via letter, SMS or email.
- Consider not putting banking details on your invoices - rather ask customers to phone you to check the details they have.
- Use bank-defined beneficiaries for online banking where possible.
- Before making payment to a supplier's bank account after receiving an emailed invoice, check that the bank account details on the invoice are genuine.
- If you receive any instructions to change banking details from a supplier, call them to verify.
- Check with your insurers if you can get cover for this risk.

Phishing

One of the oldest, most pervasive cyberthreats and a major source of stolen credentials and information, phishing is a cyber-attack aimed at stealing sensitive information like usernames, passwords and credit card details, typically using deceptive emails or websites, apparently from trusted sources, that contain malicious attachments or links to viruses or malware.

Phishing is linked to an estimated 90% of data breaches and causes not only direct financial losses but enables other forms of cybercrime.

Cyber extortion and ransomware attacks

Cyber extortion involves cybercriminals using digital methods to threaten or extort victims for money and/or assets. It often involves the attacker threatening to reveal embarrassing personal information, delete important data, sabotage systems and networks, or launch distributed denial-of-service (DDoS) attacks.

An increasingly popular type of cyber extortion is ransomware, a malicious software that locks users out of their own data, business systems and devices by encrypting their files. Victims must pay a ransom to have their files decrypted and regain access.

Such attacks can be extremely costly to businesses with substantial financial losses incurred due to ransom payments and recovery efforts, as well as downtime, lost production, and reputational damage.

Ask your accountant for help in preparing a business continuity and disaster recovery plan so you are prepared if the worst happens.

Online scams

Online scams take advantage of users' poor levels of digital literacy to lure them with false promises. Below are the most common online scams increasingly prevalent in the African region.

- Advance payment scams - fraudsters ask for financial deposits and then fail to deliver goods or services.
- Shopping scams - criminals deceive online buyers to pay upfront and then receive counterfeit items or nothing at all.
- Romance scams - criminals create a false social media identity and build an emotional connection with a victim, with the aim of soliciting money or gaining access to personal accounts.
- Tech support scams - criminals posing as representatives from technology companies offer technical assistance to gain access to users' computers and extract valuable data such as passwords and financial information.
- Cryptocurrency scams – criminals entice investors into buying fake currencies.

Banking trojans and stealers

These malicious software programs are spread through phishing emails and malicious websites to steal sensitive information such as usernames, passwords and financial data by capturing keystrokes or stealing login credentials from unsuspecting victims. Cybercriminals may use the information to steal money directly from the victim or sell the information on underground markets.

What are the risks?

According to the 2022 SHA Specialist Risk Review, cybersecurity ranks third on the list of top threats for local businesses, after power disruptions and labour matters.

The report says that not addressing cybersecurity opens companies to a range of risks, including:

- the financial loss of payments made into incorrect accounts due to BEC;
- the financial impact of business interruption due to a cyberattack;
- the financial impact of having to pay a ransom;
- the legal consequences that follow a breach of confidential or personal information;
- the reputational consequences that may impact a company's share price and brand.

How to prevent becoming a cybercrime victim

- Keep applications, software and operating systems (OSs) updated with the latest patches.
- Use and keep updated preventative anti-virus and anti-malware protections, software and protocols, as well as data encryption, firewalls and email filters.
- Use long, complicated passwords and change them often.
- Always double check you're really on the right website or app. Only download apps from trusted app stores.
- Use **YIMA**, a website vulnerability scanner, to do website security checks for scams, known vulnerabilities and security headers.
- Register for 3D Secure to secure your card details and use secure payment portals with two-factor authentication (2FA).
- Backup your system and other important files, and store on a separate device not accessible from the network, like an external hard drive.
- Beware of phishing emails. If an email looks suspicious, verify the email's legitimacy by contacting the sender directly.
- Do not click on links or icons in suspicious or unsolicited emails, and do not reply - delete immediately.
- Be careful when clicking directly on links in emails or opening email attachments, even if the sender seems legitimate.
- Don't fall for any offer that seems to be too good to be true - it usually is.
- Never provide your password, credit card or other financial information, or control of your computer, to a third party who calls unexpectedly.
- If you suspect you are being targeted by a scammer, stop all communications immediately and report it.
- If you click on a harmful link, immediately disconnect your device from the internet by unplugging your network cable or disconnecting from the Wi-Fi, then run a full anti-virus scan.
- Regular, mandatory cybersecurity awareness training for all employees is crucial to keep everyone informed about the latest cybercrime techniques.

October is Cyber Security Awareness Month – Stay Alert!

Your Tax Deadlines for October 2023

- 6 October - Monthly Pay-As-You-Earn (PAYE) submissions and payments
- 30 October - Excise Duty payments
- 31 October - Value-Added Tax (VAT) electronic submissions and payments & CIT Provisional payments where applicable.

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