WITH COMPLIMENTS

Susan B Cohen
Attorneys, Notaries & Conveyancers

Susan Barbara Cohen *BA LLB LLM (Property Law)*
Karlien van Graan *B COM LLB*

79 - 11th Street
Parkmore, SANDTON
P O Box 781622
2146

Tel: 011 883 4601
Fax: 011 883 2684
Email : susan@susancohen.co.za
Website: http://susancohen.co.za

In this Issue

Neighbours Behaving Badly: Illegal Buildings and Demolition Orders

Suing a Degree-Forging Employee for R2.2m

Tell All Your Creditors When You Change Address! The

February 2023

Neighbours Behaving Badly: Illegal Buildings and Demolition Orders

"The approval of building plans is not a mere formality in town planning and compliance with building standards promote public safety ... The courts

Case of the Summons Served on a Complex Security Guard

Check All Emailed Bank Details for BEC ("Business Email Compromise") Frauds

Budget 2023: The Minister of Finance Wants to Hear from You!

Legal Speak Made Easy

should not permit landowners to erect illegal structures on their land and then present the authorities with a fait accompli created by their illegal actions" (Extracts from judgment below)

What do you do if your neighbour starts building next door without municipal plans? A recent High Court decision confirms your right to apply for demolition.

The pensioner who built an apartment block illegally

- A property owner decided to build a multi-story block of eight apartments on his land. According to media reports he is a pensioner who spent his R900,000 pension payout on the project and planned to live off the resultant rentals of some R40,000 p.m.
- The building, which he had told his neighbours was just going to be a garden cottage, was illegal on four counts –
    - No building plans were approved by the local Council,
    - The structure encroached on building line restrictions imposed in the Town Planning Scheme,
    - The structure did not comply with the zoning of the property,
    - A restrictive condition in the title deed was contravened in that the title deed permitted only one dwelling on the property and the owner was erecting a second.
- The owner failed to comply with two "stop building" orders from the Council. Then he undertook to cease the works but instead accelerated them.
- Two of his neighbours urgently applied to the High Court to interdict further building, and the Court ordered the owner to demolish the building.
- The owner appealed this order to a "full bench" of the High Court asking for the demolition order to be postponed whilst his application to the Council for rezoning and removal of the restrictive conditions was finalised.
- Although the Council had approved the rezoning of the property it had specifically noted that it did not condone the partly constructed building, which was illegal because no building plans had been approved and the building encroached on the building lines.
- The neighbours, held the Court, had standing to apply for a demolition order, in that although their land had not been encroached upon, their rights had.
- In deciding to exercise its discretion in favour of demolition, the Court noted that the neighbours had taken steps to protect their rights immediately it became apparent that the owner was not constructing a garden cottage but an apartment block. They reported the illegal structure to the Council, and it weighed heavily with the Court that the owner carried on building even when he knew it was an illegal structure.
- The owner must demolish the building.

Bottom line – if your neighbour starts building illegally, take immediate action!

Suing a Degree-Forging Employee for R2.2m

"Oh, what a tangled web we weave when first we practice to deceive" (Sir Walter Scott, quoted in the judgment below)

It's a sad fact of life in today's business world that as an employer you must

remain constantly on guard against the dangers of “CV fraud”.

First prize of course must always be prevention – verify all claimed qualifications and work experience, accept nothing on trust. But if you do get caught out, our courts will help you if they can, as witnessed by a recent High Court case.

The “graduate” who forged a B.Sc degree

- An employee was found to have been employed, and to have been accepted into his employer’s graduate development programme, on the basis of forged qualifications in the form of a forged B.Sc degree (in Chemical Engineering) and a falsified academic record.

- His fraud was only discovered after some 8 years, and when he resigned (after disciplinary proceedings against him began) his employer reclaimed the +R2.2m it had paid him over the years.

- The employee objected, claiming that he had provided value to his employer in his work. The Court was unimpressed, no doubt at least in part because of the employer’s evidence that, as it was a bulk supplier of water to millions of people, having an unqualified person working for it (performing calculations on the type and quantity of chemicals to be added to the water) “could potentially have incredibly serious consequences for the general populace.”

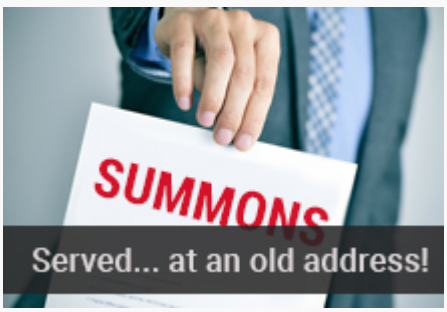
“Fraud unravels everything” – goodbye R2.2m and a pension fund

Held the Court (quoting from a well-known English case on fraud): “No court in this land will allow a person to keep an advantage which he has obtained by fraud. No judgment of a court, no order of a Minister, can be allowed to stand if it has been obtained by fraud. **Fraud unravels everything**.” (Emphasis added)

The employee, said the Court, “set out to deceive and wove his web accordingly. He achieved his goal. He has now become entangled in a web that he alone devised and cannot now be heard to complain of the consequences that must follow.”

Not only must he now repay every cent of the R2,203,565.04 he earned through his fraud, plus interest, but his pension benefits (which are normally secure from creditor claims) can be used for the purpose. To rub a final dose of salt into his wounds, he must also pay legal costs on the punitive attorney and client scale – no doubt the Court’s findings as to his untruthfulness as a witness contributing to that result.

Tell All Your Creditors When You Change Address! The Case of the Summons Served on a Complex Security Guard



“In my view, given the difficulties of a sheriff or his deputy accessing a security complex in the absence of the occupant for the purposes of service in terms of rule 4, service of process by way of it being handed to the security guard at the complex, a responsible employee older than 16 years, is valid and effective service on the debtor.” (Extract from judgment below)

Moving house (or office) will mean a busy time and a long “to do” list.

Here’s an action item to add to the “Priority” section of your list: **Give notice, in the**

required format, to everyone you have contracted with. Otherwise you could well, like the debtor in this case, wake up one morning to find your bank account frozen. Or the Sheriff of the High Court knocking on your door with a Warrant of Execution against your property.

Why is your "domicilium citandi et executandi" so important?

A "*domicilium citandi et executandi*" ("*domicilium*" for short), is a bit of Latin wording you will see in many agreements, and in simple terms it's the address you nominate in a contract where legal notices may be sent to and legal process (such as a summons) served on you.

As we shall see below, it's vital to take it seriously, both when you initially choose an address in the contract, and if/when you later move.

Debtor's bank account frozen after summons served on a complex security guard

- An occupant in a security complex with "many" residents bought a motor vehicle on instalment sale agreement, specifying his residential address as his *domicilium*.
- Eventually after he surrendered the motor vehicle it was sold on auction and he was notified to pay the balance of R108k plus interest.
- When he moved to another security complex, he phoned the creditor to advise his new address. Critically however, he didn't follow that up with a formal advice of change of *domicilum* in the required format.
- When the creditor issued Summons, the Sheriff tried first to serve it at the new address but failed when that complex's security guard said the debtor was not yet living in the unit, although his possessions were there.
- The Sheriff then served the Summons at the old address (the debtor's chosen *domicilium*), by handing it to the complex's security guard.
- Unsurprisingly there was no notice of intention to defend from the debtor, whereupon the creditor took a default judgment and attached and froze the debtor's bank account (leaving him, so he said, unable to pay his covid-related hospital and medical expenses).
- The debtor asked the High Court to set aside ("rescind") the judgment, arguing amongst other things that the summons hadn't been properly served on him.

Why the debtor lost

- As the Court put it: "Service on an address chosen by a debtor as the *domicilium citandi et executandi* constitutes good service even if the debtor is known not to be residing at the *domicilium* address, is overseas or has abandoned the premises." **In other words the summons is considered properly served whether you are still at the address or not.**
- "The manner of service at a *domicilium* address, however, must be effective. It must be such that the process served at the *domicilium citandi et executandi* would, in the ordinary course, come to the attention of and be received by the intended recipient."One way of meeting that requirement is to serve the process on a "responsible employee" – and, held the Court, security complexes not being easy to access in the absence of an occupant, it made no difference that the security guard in question worked not for the debtor but for the complex.
- The obligation is on a debtor changing address "to update or amend the debtor's chosen *domicilium* address with the credit provider." You have only yourself to blame for the consequences if you forget to do that.
- Critically, you must advise a change of *domicilium* in whatever manner the

contract requires (usually in writing at the very least). Make sure you specify it is your *domicilium* address that you are changing – "A change in residential address does not serve to change a *domicilium* address."

- And don't think that your obligation to notify a change of address falls away once the contract is terminated. On the contrary, "the *domicilium* address survives cancellation of the agreement."

End result – the judgment stands and the debtor must cough up.

Keep proof!

First prize of course is to avoid any disputes with the other party in the first place, but bad things happen to even the most careful of us so make sure that you aren't left blissfully unaware of any notices or summonses that are issued against you at the wrong address. And if you do find yourself applying for a default judgment to be set aside, make sure you have kept proof that you notified the other party of your change of *domicilium* in the specified format.

Check All Emailed Bank Details for BEC ("Business Email Compromise") Frauds

"…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." (Extract from judgment below)

Before you make any payment to a supplier's bank account on the basis of an emailed invoice, check that the bank account details in the invoice are genuine.

If your supplier's or your email system have been hacked in a BEC ("Business Email Compromise") scam, the invoice details could easily be fraudulent and if so you will be paying into a scammer's bank account.

Property transactions are prime BEC targets, but not the only ones!

You will have seen many warnings about the global problem of conveyancing email scams, where emails are intercepted and false bank account details appear in invoices or in the mails themselves. Property sales are usually high value transactions and thus a natural target for fraudsters.

Increasingly though, other non-property related business-to-business and business-to-customer transactions are being targeted – the higher the value of the deal, the more likely it is to be subjected to online crime.

Let's take a topical example…

It's high-value inverter time, and the bad guys are taking note…

You decide to install a high-value inverter, courtesy of Eskom's "no end in sight" loadshedding. Inverter installers – let's call them "Speedy Sparkies Inverter Systems" - email you a quote for R145,000. You accept. Back comes an emailed invoice from fred@speedysparkies.co.za asking you to pay R100,000 upfront to cover materials. You transfer R100k to the X Bank account on the invoice and ask when they will install. The friendly return email reads "Thanks for the payment, we'll fit you in next week Thursday. Best, Fred".

Thursday rolls around but no Fred. You phone him. “But you haven’t paid us yet” says Fred. “Yes I have, I paid into your account last week and you emailed confirmation of receipt of payment”. “No, definitely no payment received and no email from us confirming receipt.” “That’s impossible Fred, I have your email in front of me”. At which stage you notice, with a sinking heart and rising panic, that that last email came from fred@speedy-sparkies.co.za – with a hyphen. “Nope, really sorry” says Fred, “there’s no hyphen in our email address and we bank with Y Bank not X Bank. You’ve been scammed. We’ll try to help you but you need to pay the R100k again before we can install”.

Denial, anger, acceptance, then off to the bank to ask for help and off to SAPS to lay charges. Your bank and the police are sympathetic but not hopeful of recovery. So what happened?

How did you just lose R100k?

Using phishing tactics, the scammers hacked into Speedy’s email system then monitored all their emails, waiting for a high value contract to pop up. They pounced, intercepted the email to you with the invoice, changed only the return email address and the bank account.

You suspected nothing – the look and feel of the email and invoice are totally genuine, the wording of the mails is Fred’s (right down to his trademark sign-off “Best, Fred”), the email address difference is so subtle you don’t notice it. Sometimes scammers can even "spoof" an email address, where the sending email address appears to be the same as the legitimate one.

It all looks 100% authentic and of course by the time you and Fred realise anything is amiss, your money is long gone.

The only winners here are the scammers and the question now is “who is the loser?”

Who takes the loss? Who pays for your inverter now? Can you sue?

Here’s the rub – you blame Speedy for allowing their system to be hacked. You accuse them of negligence and of failing in their duty to keep your data safe in compliance with POPIA (the Protection of Personal Information Act). But Speedy deny fault and say you carry the risk and anyway it’s your mistake for not noticing the falsified email address and for not phoning Fred to check the bank account details. Speedy’s insurers confirm they have no cover for this sort of fraud.

Do you have a legal claim against the business? There’s no cut-and-dried answer to that, with our case law outcomes to date tending to vary with each particular set of facts, and the courts referring to various questions of proving negligence, compliance with payment instructions, “considerations of legal and public policy”, and reference to a general rule that anyone making a payment to someone else is required to check that they are paying into the correct account.

So **as a customer**, it’s probably safest to work on the basis that you could well be held to be the party at risk and will almost certainly have to prove (at the very least) negligence on the part of the business in order to stand a chance of establishing any claim against it.

As a business on the other hand, your legal position is far from secure. You will be accused of negligence (and perhaps also breach of POPIA) if it is your system that was hacked. Even if it is your customer’s email account that has been hacked you are still at risk, as confirmed by the recent High Court award of R5.5m (plus interest and costs on the punitive attorney and client scale) in just such a case against a conveyancing firm on the basis of its legal duty of care towards a property purchaser, and on a finding that “but for the negligent transmission of its account details and failure to warn [the buyer] upfront of the inherent danger of BEC, she would not have suffered the loss.” In the Court’s words “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”.

On a strictly practical level, your reputation is at stake and those 5-star Google Reviews could be in for a knock.

Bottom line - take legal advice specific to your case. Perhaps you will both be advised to cut your losses and to share the pain 50/50. Far from ideal, but a lot better than protracted and bitter litigation.

Prevention being as always a lot better than cure, we share below some ideas on how to protect yourself from this sort of cyber fraud in the first place.

Prevention – here's what to do

- **Businesses:** Most importantly, protect your systems from being hacked! Train all staff in the increasingly sophisticated nature of phishing emails, update all your software and beef up your anti-virus and anti-malware protections and protocols. Consider not putting your banking details on invoices and tell customers to phone you to check any details they are given. Consider using a secure payment portal with two-factor authentication (2FA) and protect any PDF documents you send (it's a myth that PDFs can't be altered). Tell customers on every email that you will never advise any change of bank details by email. Check with your insurers whether you can get cover for this risk.

- **Customers:** Take the same strong anti-hacking measures. Never pay anything without checking bank details direct with the business, either in person or telephonically (don't use the phone numbers on the emails or invoices, they could easily have been faked as well). Check email addresses carefully – make sure the return address is the same as the sender's address (some tips on how to do that **here**), watch for subtle changes like '.co.za' becoming '.com' or vice-versa, and remember that every hyphen, every letter and every number in the email address counts. Use bank-defined beneficiaries for online banking where possible. Be very suspicious of any "we've changed our banking details" communications.

Budget 2023: The Minister of Finance Wants to Hear from You!

"Finally, we pay tribute to the millions of South Africans, whose resilience and courage during these times of pandemic and economic hardship, is an inspiration to all of us who have the privilege to serve in the public sector." (From the 2022 Budget Speech)

Finance Minister Enoch Godongwana has invited the public to share suggestions on the 2023 Budget he is expected to deliver on Wednesday 22 February 2023.

Go to National Treasury's "Budget Tips for the Minister of Finance" **page** and fill out the online form.

Legal Speak Made Easy

"Waive the benefit of excussion"

Here's a phrase you will often find in suretyship documents. You as surety "waive the benefit of excussion" ("*beneficium ordinis seu excussionis*"). By

waiving the benefit, you allow the creditor to demand full payment from you without first trying to recover from the principal debtor (the person or entity who actually incurred the debt). In other words, if the debtor defaults, you are immediately as much in the firing line as the debtor itself.

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