

SOUTH AFRICA / JUDGMENT

# Simply Africa Trading (Pty) Ltd v Securitas Technology (Pty) Ltd (2021/5691) [2025]

## ZAGPJHC 61 (13 January 2025)

[2025] ZAGPJHC 61

## COURT

South Gauteng High Court, Johannesburg

## BEFORE

Fisher

## CASE / FILE NUMBER

2021/5691

Source: saflii.org · Research copy typeset by Esheria. Not court-issued or certified.

## Source record

REPUBLIC

OF SOUTH AFRICA

IN

THE HIGH COURT OF SOUTH AFRICA

GAUTENG

LOCAL DIVISION, JOHANNESBURG

Case

Number: 2021/5691

(1)

REPORTABLE:

NO

(2)

OF

INTEREST TO OTHER JUDGES: NO

(3)

REVISED:

NO

13/01/2025

In

the matter between:

SIMPLY AFRICA TRADING

(PTY) LTD Applicant

(Reg.

No. 2001/130904/07)

And

SECURITAS TECHNOLOGY

(PTY) LTD Respondent

(Reg. No.

2005/001214/07)

**JUDGMENT**

FISHER J

**Introduction**

- [1] This case involves a trial action concerning a claim by the plaintiff, in contract, for damages sustained by it as a result of a robbery at the warehousing premises in respect of which the defendant was obliged to offer remote security monitoring services.
- [2] The plaintiff claims, in the alternative, damages on the basis of delict.
- [3] There is no dispute about the written terms of the contract save that the plaintiff argues that, on a proper construction of the contract, it included the obligation to provide monitoring services in respect of a server rack/cabinet on the premises.
- [4] The defendant denies that its obligations extended to the monitoring of the server rack. It argues that the monitoring and alarm trigger devices which were installed in this server room where the rack was kept were for the defendant's benefit in that the equipment housed in the server room belonged to it and it wished to monitor it.
- [5] An important consideration is that the contract contains an exemption clause in terms of which the liability of the defendant is excluded, save in the event of gross negligence or fraud.
- [6] The defendant has pleaded a counterclaim on two bases: the first being a claim for contractual damages arising from the alleged repudiation of the contract; the second is a claim for the value of the defendant's equipment which was taken from the server room on the basis that the plaintiff had the obligation under the contract to keep this equipment insured but failed to do so.
- [7] The issues before this court relate only to the respective liability of the parties. The quantification of the damages and a point relating to locus standi are issues conveniently held over for later determination. Accordingly, the issue of liability was separated under rule 33(4) to be determined first.
- [8] I now turn to the salient facts which emerge from the evidence adduced at the trial.

**Salient facts**

- [9] The starting point is the nature and scope of the contract.
- [10] The defendant is a company that offers, inter alia, remote monitoring of premises. The plaintiff is a company that deals in the sale of export grade alcoholic beverages such as spirits and other alcoholic drinks.

- [11] The premises on which the warehouse used by the plaintiff to store the bottles of alcoholic beverages was situated was the subject of the contract.
- [12] The parties agree that the contract comprises a master agreement, various site schedules that set out the services provided and the equipment leased for the purposes of the carrying out of the services, and a document that sets out the standard operating procedures (SOPs) which the defendant is obliged to follow in the event of the trigger of an alarm.
- [13] The services are merely described as “remote monitoring of close circuit television alarms”. There is no detail provided beyond this wide description. This lack of detail has led to the dispute as to whether the server room in issue was included in the monitoring obligations under the agreement.
- [14] The plaintiff leased from the defendant the equipment as reflected in each site schedule which provided the means for the performing of the services. The defendant makes the point that the equipment pertaining to the disputed services is not part of the equipment leased by the plaintiff under the contract. This is not disputed.
- [15] Pertinently, the contract reads that the defendant does not warrant or guarantee that it or its services, personnel or equipment would be able to minimize or prevent any loss or damage to the plaintiff.
- [16] Furthermore, it was agreed that the services and equipment provided in terms of the agreement were not intended to be an alternative to or supplement any insurance.
- [17] The contract contained an exemption clause to the effect that the defendant would not be liable to the plaintiff for any loss or damage which the plaintiff may suffer or incur as a consequence of utilising the services and/or the equipment unless such loss or damage was directly attributable to the defendant's gross negligence or its fraudulent intent.
- [18] In the event of an alarm activation which led to a suspect or suspects being noted to be on the site, the operator in the control room was obliged to review the event to identify what caused the alarm and then “go live” to view the actions of the person who triggered the alarm. The operator would then perform audible warnings.
- [19] It was explained by Mr Justice Ramhali, who testified for the defendant and who was the control room operator when the event occurred, that the system allowed a live close circuit television (CCTV) monitoring of the site. This live monitoring could be called up as required when activity was notified on the site in question.
- [20] Mr Ramhali explained further the alert would register on a computer screen which he was monitoring and he would then take action as per his instructions.

- [21] Mr Ramhali explained in relation to the audible warning feature that this entailed the operator giving an audible command or warning which was transmitted through speaker equipment on site so that the suspect could be deterred. The speaker was not a two-way speaker and did not allow communication with the person detected on site.
- [22] It was agreed in terms of the SOP that, if this audible warning did not deter the suspect, the plaintiffs armed response company would be notified so that its guards could be dispatched to intervene. If there was an actual threat, the South African Police Services (SAPS) would be notified. It was agreed further that the operator would make contact with security officers on site if possible and would then continue to 'patrol' the site.
- [23] The use of the word 'patrol' in this context meant a virtual remote monitoring of the scene.
- [24] Once this protocol had been carried out, there would be a follow-up by the control room as to what had occurred and, lastly, the client would be informed telephonically of the incident.
- [25] The premises consisted of a large warehouse and some personnel offices and facilities (the buildings). The buildings were situated within a perimeter security fence.
- [26] The entrance from the perimeter onto the premises was also manned during office hours, which were 08h00 to 17h00, by a guard stationed at a security check-point inside the perimeter. This guarding service was independent from the defendant.
- [27] The plaintiff also employed an armed response company, again separate from the defendant. This alarm system allowed for the manning of the warehouse alarm to be operative overnight. Importantly, it also had a panic button feature which allowed a panic call to be sent during office hours.
- [28] Mr Emerson Haupt was the general manager of the defendant at the time of the incident. He has more than 20 years of experience in the security industry on the technical side in relation to remote monitoring. He testified for the defendant.
- [29] Mr Haupt explained that the services offered were the monitoring of the perimeter of the premises after hours. He explained that this entailed the installation of cameras around the perimeter which would be aligned with movement detectors in the form of an invisible beam. This system was operational only after office hours.
- [30] The only monitoring alarm system which was in operation during office hours was the system in question in the server room. The server was an integral part of the remote monitoring system.
- [31] The server was housed in a server cabinet/rack. The cabinet had a glass door.
- [32] An alarm was installed in the sever rack which operated on the basis that it was triggered if the door was opened. This was referred to as a "quad alarm".

- [33] There was a further protection which entailed a signal being sent to the control room if the If the server was unplugged or the connection to the server failed for any reason. This was called a “loss of site” alarm.
- [34] The protocol for loss of site was that there would be a telephone call placed by the operator to the client to determine what had occurred and if this could not be established the armed response company and the police would be called.
- [35] Mr Haupt testified that the quad alarm was for the benefit of the defendant only in that it protected the defendant’s equipment. The equipment value is approximately R80 000.
- [36] He testified further that the loss of site alarm served to notify that there had been a technical interruption of the operating system. This was as opposed to the alarm which was triggered when the server rack door was opened.
- [37] The loss of site alarm would occasion inquiry by way of telephone call and if this could not be achieved there would be a notification of armed response company and police. The argument of the defendant was that this facility protected the client so contact could be kept with the client at all times, whereas the door alarm of the server cabinet was for the defendant’s benefit alone.
- [38] Thus, in sum, the following systems were operative during office hours: An on-site security guard; panic buttons which connected both the defendant and the independent security company that offered armed and tactical response; and the quad alarm.
- [39] It is not disputed that the quad alarm system was not part of the equipment leased by the plaintiff under the agreement.
- [40] Mr Prestin Cheslin Aitkin who was the only witness for the plaintiff was in charge of the warehouse on the day in question being 26 September 2016. He described how the robbery unfolded and also testified as to his usual procedure in relation to the alarm systems in issue.
- [41] As usual Aitken arrived at the warehouse just before 08h00. As part of his employment Aitken had in his possession a remote-control device that operated the perimeter gate at the entrance to the premises.
- [42] The gate was palisade in nature and was controlled remotely by Aitken with the remote-control device. Once opened and closed behind him Aitken would give the remote control to the guard who manned the security check-point.
- [43] Aitken on the day, as he did in the normal course attended on the warehouse; disarmed the alarm system which he had armed the evening before when he left the premises.
- [44] Aitken was the person who opened the offices each morning and locked up at night.

- [45] There were nine other staff members who performed various functions that the packing, loading and off- loading of the alcohol crates involved.
- [46] The morning began in the normal way. At approximately 08h30 three armed men wearing reflective vests labelled with the word “POLICE” entered the offices. They initially pretended to be policemen but it soon emerged that they were robbers.
- [47] The robbers proceeded to round up the staff, including Aitken and the security guard. They then used cable ties to handcuff them with their hands behind their backs. All had their mobile phones confiscated. They were told not to swich them off however.
- [48] During the course of the action, Aitken’s mobile phone rang. The robber who seemed to be in charge of the proceedings pointed his firearm at Aitken and instructed him to take the call and to “speak nicely”.
- [49] The call was from the Director of the plaintiff Mr David Kaplan. It was a business-related call.
- [50] Aitken, at gun-point, did he was told and pretended to Kaplan that nothing was amiss. He was later praised for his “co-operation”
- by the gun wielder.
- [51] The next demand was that he take the gun-wielder to the server room. He duly complied – at gunpoint.
- [52] Aitken understood that the reason why access to the server was required by the robbers was an attempt to thwart the security
- measures that were in place.
- [53] When access to the server room was gained , Aitken was confronted by another man. This man was masked with a face mask that covered most of his face and he wore a beanie hat and he wore gloves.
- [54] Aitken referred to this man as “the IT Man” because he appeared to understand the technology of the server and seemed to know what he had to do in relation to the server.
- [55] As I have said, the server rack was a steel up-right cabinet with shelves on which the server was placed and it had a glass door. The IT man opened the glass door to the rack
- [56] At this point it is important to understand what was triggered on the system by the opening of the door. I move then to analyse how the system operated.
- [57] The opening of the door to the server rack triggered what was referred to as a quad-alarm in the defendant’s control room.

- [58] This trigger manifested as a line-item pop - up on a computer monitor screen which, when clicked on took the person monitoring the screen to a page containing four photographic images positioned on the screen in postcard size quadrants. The screen measured 22 inches.
- [59] The two top and bottom left photographs were still snapshots taken at one second intervals. The fourth was a moving composite of the three forming a moving montage. The aim of this system was to give a snapshot view of who had opened the cabinet.
- [60] The court was provided with copies of the view which appeared on the screen so that it could assess for itself what emerged therefrom.
- [61] Aitken was shown standing in the server room with his back to the camera and his hands behind his back. He was looking on at the masked man who had opened the server door. The man was wearing a beanie hat and gloves.
- [62] Aitken confirmed that the man depicted at the cabinet was who he referred to as the IT Man. The gloves he says were long and made of a thick material. After having shown the men to the server, Aitken was immediately escorted out of the room by the gun-wielding man back to the office where all the employees were being held. The gun-wielding man was not visible on the screen.
- [63] Ranhali testified that this alarm registered on his screen as low priority. He had not been instructed to respond to this alarm other than to check what had caused the trigger. He denied that he had the obligation to take any action if he was satisfied that there was nothing suspicious taking place.
- [64] He surveyed the snapshots which appeared on the screen. He recognised Aitken. He could not discern the cable ties. They are not readily visible on the photographs which were placed before the court. To my mind there is nothing which should have evoked Ranhali's suspicion.
- [65] The fact that the man attending to the server was masked did not attract Ranhali's interest in that it was lockdown and everybody was required to wear masks. The fact that the person was gloved likewise did not cause suspicion because it was winter.
- [66] Furthermore, the opening of the server door was not an isolated occurrence. There was undisputed testimony that the opening of the server door had previously occurred over the preceding months on least three other occasions.
- [67] The reason for the opening of the server door on these occasions was that the plaintiff's personal internet device (i.e.it was not connected with the defendant's system) was giving trouble which required it to be rebooted. The device was stored in the same cabinet as the server and, thus, to access the plaintiff's device the glass door had to be opened.

- [68] Mr Haupt testified that the plaintiff was not strictly allowed to store its own equipment in the server rack precisely because of the nuisance factor involved. It seems it was overlooked however.
- [69] Mr Rankali knew that the plaintiff's equipment was housed in the same server cabinet and that there had been at least three occasions where the door had been opened by Aitken and others to attend to this equipment.
- [70] The most contentious part of Aitken's evidence was that on each occasion, when there was such a trigger, the person monitoring the alarm would call to find out the reason for the trigger. This evidence was relied by the plaintiff for its version of the contract.
- [71] The plaintiff argues that it was practice and a part of the defendant's obligation under the contract to respond to the trigger by phoning Aitken. Had this been done, argues the plaintiff this would have resulted in either the phone not being answered which would occasion further action in the form of notification of the plaintiff's security company which may have yielded discovery of the robbery in progress or in Aitken being in a position to give the alert.
- [72] As it happened, the robbery progressed for more than two hours after the quad alarm was triggered. It involved further robbers bringing trucks into the loading area and even using the fork-lifts at the warehouse to achieve the loading of the cases of drink. The fork-lift driver was ordered at gun-point to perform the loading.
- [73] A substantial amount of alcohol was stolen in this well-orchestrated heist. The plaintiff alleges it suffered damages in an amount of in excess of R8.7 million due to the loss of its stock. As I have said, the quantum is not part of this inquiry.

## Discussion

- [74] Essentially, the dispute under the contract is whether the plaintiff was entitled to 24-hour protection of the server which would require action on the part of the defendant or whether it was a facility for the defendant only.
- [75] It is clear that the main service offered by the defendant was an after-hours monitoring of the perimeter of the premises. This required arming at the end of the working day and disarming at the start of the day.
- [76] During the day there were other security measures in place comprising the security guard and panic buttons which were person- activated.
- [77] The question posed when weighing up the probabilities is why only the server alarm was armed 24/7.
- [78] It is not in dispute that there was no other armed service during the day.

- [79] Neither is it disputed that the equipment protecting the server was not leased by the plaintiff in terms of the contract as was the case with the other equipment which facilitated the furnishing of the services under the agreement.
- [80] It stands to reason that the defendant would want to protect its equipment during the day. It could, after all, not control the access that could be had to its equipment during the day.
- [81] Ranhali struck me as an honest witness. His evidence was to the effect that was not instructed to telephone and alert armed or police response in the event of a trigger of the quad alarm. This position was confirmed by Haupt.
- [82] In any event, the system under the contract was set up in such a way that there were layers of intervention which started with visual checking of the scene and escalated to armed response and police involvement in the event of the perimeter being breached. The evidence was to the effect that there would first be a visual check and if necessary (i.e. if a suspect was noted on site) the next step would be the audible deterrent. Armed response would be a last resort.
- [83] To my mind the probabilities support the defendant's version of the agreement. However, at best for the plaintiff the probabilities are evenly balanced.
- [84] However, even if it is accepted if the defendant was contracted to initiate the protocol, the initial check by Ranhali would, to my mind have satisfied a person in Ranhali's position that a threat of the type where armed response action was required.
- [85] The probabilities support the defendant's contention that the contract did not include 24-hour monitoring of the server rack. To the extent that the server was compromised the control room would be notified immediately. This ultimately occurred albeit only after the robbery was over. Thus, the plaintiff's argument that keeping this communication mechanism functional and operational was a priority which served the plaintiff's requirements is not compelling.
- [86] Thus, I find that the plaintiff has not established a breach of contract.
- [87] However, even if the contract required that Ramhali take some action, and it is not clear what action would have been appropriate in any event, his failure to act does not rise to the level of gross negligence required for liability in terms of the exemption clause. He checked the site and nothing evoking suspicion of an armed robbery was noted.
- [88] Furthermore, the submission that if action were taken this would have thwarted the robbery is fanciful.
- [89] Thus, the claim for liability under the contract must fail.

The claim in delict

[90] The plaintiff asserts that, notwithstanding the contracting out of liability for negligence, the plaintiff still can found a claim on delictual principles.

[91] The proposition is stated as follows:

“Although there has historically been some uncertainty on this score, it is respectfully submitted that the law in this regard is now clear. Delictual liability can arise even in the case where the relationship between two parties is regulated by means of a contract.”

[92] As authority for this proposition a scattergun approach is taken with bald reference to: Lillicrap, Wassenaar and Partners v Pilkington Brothers (SA) (Pty) Ltd 1985 (1) SA 475 (A) at 499 A-D; Holtzhausen v ABSA Bank Limited 2008 (5) SA 630 (SCA) at 633-634; Trio Engineered Products Inc v Pilot Crushtec International (Pty) Ltd

[2018] ZAGPJHC 447 at paragraphs 23-27.

[93] This is unhelpful. It fails to take account of the approach to Lillicrap adopted by the Constitutional Court in Country Cloud Trading CC v MEC, Department of Infrastructure Development[1].

[94] The Court in Country Cloud, in fact, warned that courts should be wary of extending the law of delict where there are existing contractual relationships. It held to do so may subvert the autonomy of parties to regulate their rights and duties. The principle was put thus by the Court:

*“Where parties take care to delineate their relationship by contractual boundaries, the law should hesitate before scrubbing out the lines they have laid down by superimposing delictual liability”.*[2]

[95] Unterhalter J (as he was) in his careful exposition of the position taken in Country Cloud in Trio Engineering Products Inc v Pilot Crushtec International (Pty) Ltd[3] concluded, correctly with respect, that the position adopted in Country Cloud would appear to exclude concurrent liability in contract and delict in that once parties have chosen to frame their relationship in contract, respect for the autonomy of the parties precludes the imposition of duties in delict that may be different and have

different consequences.

[96] The most that can be said of the authorities relied on by the plaintiff for its delictual claim is that the facts of a particular case may accommodate concurrent claims in contract and delict.

[97] Whether or not the Constitutional Court in Country Cloud meant to overrule this position is not entirely clear and it is not necessary for me to decide this. I do, however, incline to the view expressed by Unterhalter J in Trio Engineering that it does not do so.[4]

[98] What is clear, however, is that on the facts of this case, there is no room for a claim in delict.

[99] The plaintiff's reliance on *Loureiro and Others v Imvula Quality Protection (Pty) Ltd*[5] is misplaced in that that in that case the security contract in issue did not contain an exemption clause.

Order

[100] In the circumstances I order as follows:

1. In respect of the plaintiff's claim, judgment is entered in favour of the defendant,
2. In respect of the defendant's counterclaim, the plaintiff is declared to be liable for the defendant's damages to be quantified.
3. The costs of the action and counterclaim, thus far, are to be paid by the plaintiff such costs to be taxed on scale C.

JUDGE OF THE HIGH COURT

JOHANNESBURG

This Judgment was handed down electronically by circulation to the parties/their legal representatives by email and by uploading to the electronic file on Case Lines. The date for hand-down is deemed to be 13 January 2025.

Heard: 07, 08 & 09 October 2024

Heads: 05 November 2024

Delivered: 13 January 2025

APPEARANCES:

Applicant's counsel: Adv. D. Dorfling SC

Applicant's Attorneys: JHS Attorneys

Respondent's Counsel: Adv. B Boot SC

Respondent Attorneys: Weavind & Weavind Attorneys

[1] *Country Cloud Trading CC v MEC, Department of Infrastructure Development* 2016 (1) SA 1 (CC).

[2] *Id* at para 65.

[3] *Trio Engineering Products Inc v Pilot Crushtec International (Pty) Ltd* (16/16836) [2018] ZAGPJHC 61; 2019 (3) SA 580 (GJ) (22 March 2018).

[4] *Id* at para 27.

[5]

[2014] ZACC 4; 2014 (3) SA 394 (CC).

## Source & reproduction note

Judgment wording, source notices and original paragraph numbers are retained. Esheria supplies the layout and this PDF's page numbers; these are not the source pagination. This is a research copy, not an official or certified court document. Check quotations, citations and publication restrictions against the original source before relying on it.

**ORIGINAL SOURCE**      <https://www.saflii.org/za/cases/ZAGPJHC/2025/61.html>

**CASE PAGE**              <https://chat.esheria.ai/case-law/south-africa/simply-africa-trading-pty-ltd-v-securitas-unknown-topic-agpjhc-2025>

Prepared on 12 October 2026 · Esheria