



ARBITRATION AWARD

Case No. GPBC 2945/2010

Part time Panellist: Sugan V Reddy

In the Arbitration Between:

PSA obo R SOMMER

APPLICANT

AND

DEPARTMENT OF TRANSPORT KWAZULU - NATAL

RESPONDENT

ARBITRATION AWARD

DETAILS OF THE HEARING AND REPRESENTATION

1. The arbitration of this dispute commenced on 24th June 2016 and was thereafter set down for arbitration on 05th August 2016, 02nd September 2016, 10th March 2017, 18th August 2017, 05th April 2017, 18th October 2018, 29th March 2019, 01st August, 10th September 2019 and was finalised on 18th September 2020 . The arbitration was held at the offices of the Department of Transport Kwa- Zulu Natal in Pietermaritzburg. The matter did not proceed on a number of the aforesaid days, for a variety of reasons relating either to the unavailability of witnesses or to the fact that the parties hereto did not receive proper notice of the arbitration being set down.
2. Applicant, i.e. Mr Ridwaan Sommer (hereinafter referred to as 'the applicant'/ 'Applicant') appeared and was represented by Mr G Kirby-Hirst, an attorney. Respondent, i.e. Department of Transport

Kwazulu-Natal, (hereinafter referred to as 'the respondent' / 'Respondent') was represented by Ms A Lambert, also an attorney.

3. The parties hereto submitted three combined bundles of documents which were marked 'BA', 'BB' and 'BC' respectively. I ensured that the parties were, inter alia, advised that I would only have regard to documents in the aforesaid bundles of documents which were specifically referred to by them during these proceedings.

ISSUES TO BE DECIDED

4. I am required to decide whether the dismissal of Applicant was procedurally and substantively fair and if not, the relief he is entitled to.

BACKGROUND AND EVIDENCE

5. I set out hereunder only that which is necessary to enable me to determine this matter.
6. It is common cause that Applicant was employed by Respondent on 22nd October 2001. It is also not in dispute that although a decision was taken to dismiss Applicant on 17th February 2009. As at the date of his dismissal, Applicant was employed as an administrative officer. Given the provisions of PSCB Resolution No 1 of 2003 such dismissal was only implemented on 04th August 2010 pursuant to the finalisation of the appeal (upholding the decision to dismissal) by Respondent. It is apposite to state that Applicant (who was on suspension pending the disciplinary enquiry which resulted in his dismissal) resumed his duties in terms of the mandatory provisions of the aforesaid resolution given that the appeal was not finalised within 30 days (as is required by the said resolution).
7. Applicant worked at the Motor Licencing Bureau ('MLB') in Pietermaritzburg, a component/unit within Respondent. MBL performed the functions of issuing motor vehicle licences (licence discs) and processing transactions in relation to motor vehicles, eg changing the status of vehicles, (registered on its system as being unroadworthy), from unroadworthy to roadworthy thereby enabling same to be issued licences allowing same to be driven on public roads. The process of achieving this is known as a 175 transaction. This would be achieved by firstly having a deregistered vehicle tested by a private test station to determine its fitness to be driven on a public road. If the test indicated that the vehicle was fit for the aforementioned purpose the test station would issue a Certificate of Roadworthiness ('COR'/'CRW') certifying that the vehicle was fit to be driven on a public road. The owner of the said vehicle would then go to the MLB and produce a physical Certificate of Roadworthiness, i.e CRW. One of the clerks in the employ of Respondent would then process the 175 transaction utilising an electronic digital system known as the E-NaTIS (Electronic National Traffic information System). The E-NaTIS system ('the system') contains the relevant historical data of all motor vehicles, eg registration numbers, chassis number, name of owners, type of vehicle, roadworthy status, etc. Upon production of the physical CRW the clerk would enter the name and infrastructure number of the examiner who examined the vehicle and determined it to be fit to be driven on public roads, the date of the CRW test and the name of the test station at which the test was conducted. Once this information was captured on the system the vehicle's status would change (on the system) from unroadworthy to roadworthy thereby enabling the vehicle to be issued a licence. The physical CRW would be retained by the MBL. MBL outsourced the physical storage of this CRW, amongst other documents, to Document Warehouse. Document Warehouse would scan all documents, so stored, onto a system known as MGX. MLB also had access to the said MGX system and could, inter alia, access the scanned documents if it needed to

via computers and MGX software which was linked to MBL. It is apposite to point out that it is not in dispute that test stations are graded entitling them to test only certain types of vehicle, eg only light or only heavy motor vehicles on the one hand or both types of vehicles on the other. It is also important to state that the test station retained proof of CRWs ('certificates of roadworthiness') issued, either in the form of duplicate original CRWs or the stub of the original CRW which contained relevant information relating to the test, eg date of test, name or infrastructure number of the examiner and vehicle tested.

8. It is also not in dispute that in order to access and process transactions on the E-NaTIS system one had to log into same using a (personally) dedicated password and username in respect of each employee of Respondent. The username was not confidential and was accessible to any person able to access the system. The password, however, was strictly confidential to the employee to whom it was allocated so much so that the system (E-NaTIS) would prompt a user after each 30 (thirty) day cycle to create (for the purpose of accessing the system) a new password. A password could not be used for more than a period of 30 days. Applicant signed a 'NaTIS USER UNDERTAKING' the relevant details of which are set out in the 'charges' referred to hereunder. The allegations against Applicant arose from the processing of 4 (four) 175 transactions. It is not in dispute that 2 (two) of these transactions were processed on 24th August 2007 and the others on 06th and 17th September 2007 respectively, days when Applicant was at work. Of importance and not in dispute either, is that Applicant's password changes (relevant to the 30-day password change cycle) occurred on 03rd August 2007 and 12th September 2007.
9. It is not in dispute that people coming to the MLB in order to obtain vehicle licences via the 175 transaction dealt with clerks at counters. Licences could be issued fraudulently utilising the system. A clerk could access information, randomly, from any one of the CRWs used in regular 175 transactions, eg names and infrastructure numbers of examiners and names of test stations. These details could be used to process fraudulent 175 transactions to enable the licencing of a vehicle which did not have a CRW and which was reflected as being unroadworthy on the system. In this regard the foregoing details would enable/support the entry of a CRW onto the system thereby entitling a licence to be issued. In this regard it has to be stated that Applicant submitted that a fraudulent CRW could be used to succeed in having a 175 transaction successfully processed. It is convenient to point out that, in the absence of a (physical) fraudulent CRW being scanned, it in all probability ought to have been located at and retrieved by Respondent from Document Warehouse which stored same unless it also was not sent to the said Warehouse.
10. It is not in dispute that Applicant had his own office. It is apposite to state that Applicant's unchallenged version is that he did not have the equipment in his office to process a 175 transaction. Respondent's evidence, however, that Applicant could "log in" at his workstation also went unchallenged. Furthermore the unchallenged evidence of van Straaten is that one of the four impugned transactions was processed at Applicant's workstation. The parties also agreed that there was nothing untoward when Applicant logged in [to the e-Natis] on different terminals.
11. It is common cause that the 'charge' which Applicant faced, was found guilty of and which led to his dismissal reads as follows:

'The misconduct which you allegedly committed is that you:

1. Were negligent.
2. Failed to carry out a lawful order without just or reasonable cause.

3. Contravened paragraphs C4.4; C4.9 and C4.12 of the code of conduct for the Public Service:
C4.4 Executes his duties in a professional and competent manner.
C4.9 Promotes sound, efficient effective, transparent and accountable administration.
C4.12 Honours the confidentiality of matters, documents and discussion, classified or implied as being confidential or secret.

4. Prejudiced the administration, discipline and/or efficiency of the Department, office or institute of the state.

In that

Despite signing NaTIS User Undertaking on 18 January 2007 which stipulates the following:

- 4.1.7 to be liable for all transactions or actions conducted under my NaTIS User Number.
- 4.8.1 Not to disclose my NaTIS User password to any other Person or allow any other Person access to the System whilst logged on with my user number and password.
- 4.1.9 to activate a screen saver or not to leave my Workstation unsecured or unattended without logging off.
- 5.1.13 to exercise all reasonable skill, care and diligence in the discharge of my obligations in terms of the Undertaking and shall perform all services with the highest standards consistent with, and applicable to The Road Traffic Legislation and the objectives of the NaTIS Security Policy and Standards.

a) You changed your NaTIS password on 2007-08-13 and failed to safeguard this as evidenced by the Certificate of Roadworthiness (175) transactions which were processed over the period 2007-08-24 to 2007-09-03.

b) You changed your NaTIS password on 2007-09-12 and failed to safeguard this as evidenced by the Certificate of Roadworthiness (175) transactions which were processed over the period 2007-09-20 to 2007-09-28.'

12. The following persons testified on behalf of Respondent:

- (a) Ms Theresa van Straaten, a Senior Administration Manager at MLB, Pietermaritzburg; ('van Straaten')
- (b) Mrs Beulah Wagner, the Assistant Manager at MBL, Pietermaritzburg; ('Wagner')
- (c) Mrs Thembililhe Virginia Nzuza, Respondent's Director of Labour Relations; ('Nzuza'), and
- (d) Mr Brian Duncan Jeary, a motor vehicle examiner at PMB Roadworthy Centre; ('Jeary')

13. Applicant as well as Mr Roshan Lil-Ruthan, a senior Labour Relations Officer at the Public Servant's Association testified on his behalf.

14. It is important to set out the respective arguments of the parties at these proceedings. Respondent contends that "Sommer was charged with performing irregular transactions on the E- Natis System and irregular transactions were performed under his name." According to Respondent, I am required to determine, inter alia, whether Applicant performed any of the irregular 175 transactions and if so, what the appropriate sanction for same is. Applicant argued that "the charge, is essentially based on the issue of whether he was negligent or not in that, despite signing a NATIS user undertaking, he changed his password and failed to safeguard this as evidenced by the certificate of roadworthiness (175) transactions which were processed over the period." It is Applicant's contention (during argument) that

“the charge relates to a failure to safeguard rather than the applicant specifically performing the alleged fraudulent transactions himself.” Applicant submits (in his written argument) that “During the course of the arbitration process, it appeared as if respondent’s representative was attempting to approve [to prove] the applicant guilty of a charge akin to having performed the transactions himself on his username”. In this regard van Straaten stated that Applicant could perform 175 transactions at his workstation and testified that one of the impugned transactions was in fact performed at his workstation. She also referred to computer generated documents which reflected that one such transaction was processed at Respondents workstation. Although evidence in this regard by van Straaten went unchallenged, Applicant testified that he was unable to process 175 transactions from his workstation. Applicant’s evidence in this regard also went unchallenged. It is to be noted that all the impugned transactions allegedly processed by Applicant were processed on days when he was present at work. The evidence of van Straaten was that “you are liable for all transactions under your username and that you had to secure your password to the best of your abilities”. She testified that Applicant was guilty because the transactions were processed using his username [and password]. She stated that she could not comment, when it was put to her that Applicant denies that he performed fraudulent transactions. Applicant submitted in his written argument that the foregoing, i.e that Applicant personally processed fraudulent transactions, “was not the requirement for the charge and the issue as per the charge was whether or not there was a failure to safeguard the password.”

15. The event giving rise to this whole saga commenced when a fellow colleague of Applicant, i.e one Ms Davenport (who performed the same functions as Applicant) was advised by a fellow employee that a clerk at MLB , i.e Ms Memela had approached Davenport’s aforesaid fellow employee with a request that he/she steal Davenport’s password. Davenport reported this communication to Miss Beulah Wagner(‘Wagner’) the assistant manager at the Motor Licencing Bureau (‘MLB’) in Pietermaritzburg. Wagner then instructed Ms Theresa van Straaten (‘van Straaten’) a Senior Administration Manager to investigate possible irregular conduct at MLB, Pietermaritzburg. Respondent’s evidence in this regard is that 2 (types) of transactions processed in 2007 were investigated. According to van Straaten every transaction of these types which were processed during 2007 were scrutinised for the purpose of the investigation. Only one type of transaction known as ‘175 transactions’ were dealt with during this arbitration. This investigation led to her uncovering numerous 175 transactions, processed by 7 (seven) employees of Respondent, which she believed to be fraudulent. Employees had conducted different number of fraudulent transactions with one performing approximately 200 such fraudulent transactions. The view that the identified transactions were fraudulent had, as its basis, the inability to locate the CRWs by van Straaten, acting in concert with certain other employees of Respondent. According to van Straaten the CRWs could not be located on the MGX system nor at the storage centre where she and the other investigators personally went to and conducted physical searches for the physical CRWs relating to the said fraudulent transactions. Van Straaten also caused investigations to be conducted at the Motor Vehicle Test Stations which purportedly issued the CRWs relating to the transactions identified as fraudulent by Respondent. One of the Motor Vehicle Test Stations, i.e PMB ROADWORTHY CENTRE which purportedly issued the suspicious CRWs relating to two 175 transactions processed under Applicant’s username and password, confirmed that they did not issue same. Furthermore van Straaten stated that PMB Roadworthy Centre would not have been able to test (and issue a CRW) one of the vehicles in one of the two transactions processed under Applicant’s username and password, as same was a tipper (truck). PMB ROADWORTHY CENTRE was a B grade test station which was not authorised to issue CRWs in respect of trucks (heavy motor vehicles. According to her the physical dimensions of the said test station would have been incapable of allowing the said tipper

to be examined. She knew this because she visited the said test station during her investigations. The CRWs which were reflected on the E-NaTIS 175 transactions enabled the 175 transactions to be successfully processed. According to van Straaten, Applicant processed 4 (four) such transactions. As stated these transactions were processed on 24th August 2007, 06th September 2007 and 17th September 2007. It was agreed that evidence would be and was in fact led in respect of only 2 (two) of these transactions and that the conclusions/findings in respect of these 2 transaction would be applicable to the remaining 2 transactions. These 2 (two) transactions reflected that the vehicle tested, in respect of each such transaction, was tested by an examiner, one Jeary at PMB Roadworthy Centre. It is apposite to state that the evidence of Jeary is that he did not test these two vehicles on 24th August 2007(or at any other time), as is reflected on the E-NATIS relating to the aforesaid two transactions. It is also important to note that in respect of the other two allegedly fraudulent transactions Respondent was not able to obtain evidence from the relevant test station/s as to whether the vehicle/s were in fact tested at this these station/s as is reflected on the E- NATIS 175 transactions. It is apposite to state that the name of the examiner and test station as well as the date when the CRW was issued would (in 2007) have had to have been captured by the person processing the 175 transaction. The undisputed evidence is that Applicant's password was changed on 03rd August 2007 and 12th September 2007 respectively. Although Respondent agreed that Wagner was advised that one of its employees made enquiries relating to the theft of the password of another employee as aforementioned it maintained that there was no proof that passwords, including those of Davenport and Applicant, had in fact been stolen, thereby maintaining that the employee whose username and password appeared on any 175 transaction, which was allegedly fraudulent, processed such transaction. In this regard van Straaten stated that Applicant could perform 175 transactions at his workstation and testified that one of the impugned transactions was in fact performed at his workstation. She referred to computer generated documents which reflected that one such transactions was processed at Respondents workstation. It is to be noted that all the impugned transactions allegedly processed by Applicant were processed on days when he was present at work. Although evidence in this regard by van Straaten went unchallenged Applicant testified that he was unable to process 175 transactions from his workstation (office). Applicant's evidence in this regard also went unchallenged. The evidence of van Straaten was that "you are liable for all transactions under your name and that you had to secure your password to the best of your abilities". She testified that Applicant was guilty because the transactions was processed using his username [and password]. She stated that she could not make any comment when it was put to her that Applicant denied that he performed fraudulent transactions. It was put to van Straaten that Applicant's version would be that:

- (a) Not enough information was obtained to "conclusively" prove ("show") that these transactions were fraudulent.
- (b) Applicant "never" performed any fraudulent transactions.
- (c) If (the four relevant) transactions were found to be fraudulent Applicant did not process such transactions.

16. Applicant was employed as an administrative officer supervising approximately 40 staff, some of whom, i.e the clerks at the counter, dealt directly with the public, processing transactions which formed part of the functions of Respondent, including 175 transactions. It is Applicant's evidence that performing 175 transactions was not part of his duties. It is not in dispute that Applicant, inter alia, assisted his subordinates when difficulty was encountered by them with any transaction, including 175 transactions and that when he did so he logged into the E- Natis at different terminals and workstations using his own password and username. His evidence in this regard is that any subordinate that he was assisting would be standing alongside him when he entered his password, in the aforesaid circumstances, and

would be able to [surreptitiously] gain knowledge of his password if he/she wanted to. It is Applicant's evidence is that he was not able to process a 175 transaction from his office given that same had no access to the E-Natis system (see paragraph hereof 10 in this regard). When assisting clerks, at the counter, payment section, verification section or at "**enquiries**", he (was generally) dealing with "irate customers". These customers were sometimes brought to his office. As stated when assisting the employee who had called him such employee would be standing alongside him. His response to the question as to how often he would "log in with your password daily" was that it could be "over 10 to 20 times a day, could have been more because I was working as a verification supervisor and I had to check of on all documentation for payments for different types of transactions". I set out the evidence in this regard in some detail given Applicant's defence relating to the theft of his passwords. Applicant testified that it was difficult to conceal his laptop (when logging on to same with his password) demonstrating such difficulty by forming his arms in a shape resembling that of horns of a bull. He testified to the fact that he was assigned to put mgx documents in boxes to enable same to be taken to the warehouse so that it could be scanned to enable Respondent to have (computer) access to same. According to him the documents, which were not on the premises where he worked, were in wet boxes and "in a mess." Applicant confirmed the event concerning the report of an attempt to steal Davenport's passport stating that he thereafter assisted Wagner to secretly watch employees suspected of engaging in suspicious activity (Wagner testified that she had no knowledge of this). According to Applicant the 4 (four) impugned "could be valid or invalid but the reason we are here is because the documents could not be located." If these transactions were fraudulent he stated that they would have been performed by employees who had his username and password and that they had "criminal intent." According to him he had "never" performed any fraudulent transaction. He would not have been aware that PMB Roadworthy Centre would not have been capable of testing the tipper as the E-Natis system would not have indicated same. Applicant stated that he did not personally attend any appeal process.

17. In the event Applicant's evidence was that he had not performed the four allegedly fraudulent transactions and that same were performed by some other employee who had to have stolen [two of] his passwords. Applicant was then cross-examined. He confirmed that passwords were changed every 30 days and that any password could not be used after the period of its validity, i.e 30 days. He agreed that his username and passwords were used in the 4 (four) impugned transactions and that he signed the Natis User Undertaking. Applicant did not take issue with clauses 4.1.4, 4.1.6, 4.1.7, 4.1.8 and 4.1.9 of same at page 264 of bundle A (which was identical to a User Undertaking he had signed prior to the dates that the 4 impugned transactions were processed). He admitted that he did not always log off the system (as the Undertaking requires) stating that because of the nature of his job he had "to deal with irate customers waiting" ("..... at different areas of the office."). Applicant stated that he did not activate any screensaver because such function did not exist. Applicant admitted that did not comply with clause 4.1.9 of the aforesaid undertaking which reads as follows: '4.1. I undertake-4.1.9 to activate a screensaver or not to leave my Workstation unsecured or unattended without logging off.' It was then put to him that "In terms of this (User Undertaking) you are then directly responsible" to which applicant's response was "Yes." When questioned he responded by stating "I won't be able to say who was with me during these 4 (four) transactions." He stated that the employees with criminal intent were Memela and Mazeka who were "normal clerks."

18. It is apposite to state that although the motor vehicles involved in these four transactions were de-registered none of their owners queried their de-registration when the fraudulent transactions were discovered. It is also appropriate to state that it is not in dispute that 4 (four) of the 7 (seven) implicated employees either resigned or were dismissed, as was Applicant, but that the internal disciplinary enquiries relating to 2 (two) of the implicated employees, i.e. Memela and one Mr Mchunu had, as at the date of the finalisation of these proceedings, not been finalised and that they were still in the employ of Respondent.

19. When I sought clarity relating to the charge reflected above Respondent did not see the need for same and submitted that I am not bound by these charges and could have regard to the evidence in determining the nature of the "offences". Respondent contended that I could not disregard any evidence. Applicant contended that I could not have regard to evidence as to whether or not he processed these charges fraudulently.

ANALYSIS OF THE EVIDENCE

20.(a). Despite Applicant having been found 'guilty' of the allegations contained in the aforementioned 'charge' and having been dismissed as a result thereof, I am required to determine whether Respondent succeeded in proving the 'guilt' of Applicant (during the arbitration proceedings) in having processed the aforesaid 4 (four) transactions personally, which would mean that he acted fraudulently. The essence of the aforesaid 'charge' which resulted in Applicant being dismissed is his failure to safeguard his password despite him having signed the NaTIS User Undertaking ('Undertaking') "which stipulates the following:

- 4.1.7 to be liable for all transactions or actions conducted under my NaTIS User Number. Strict does not mean that he processed the said transactions.
- 4.8.1 Not to disclose my NaTIS User password to any other Person or allow any other Person access to the System whilst logged on with my user number and password.
- 4.1.9 to activate a screen saver or not to leave my Workstation unsecured or unintended without logging off.
- 5.1.13 to exercise all reasonable skill, care and diligence in the discharge of my obligations in terms of the Undertaking and shall perform all with the highest standards consistent with, and applicable to The Road Traffic Legislation and the objectives of the NaTIS Security Policy and Standards."

(b). The 'charge' in respect of which Applicant was dismissed and the charge of having personally and fraudulently processed the 4(four) impugned transactions are distinct and worlds apart, even to a layperson. Respondent with full knowledge of all facts which would have entitled it to 'charge' Applicant with having intentionally and fraudulently processed the aforesaid 4 (four) transactions and with the ability to state that that was in breach of the Undertaking chose instead to 'charge' Applicant with the failure to safeguard his password in breach of the Undertaking setting out aspects of same which it obviously considered to be pertinent and/or to such failure. The most plausible inference is that, being alerted to the attempts to steal passwords or at least having received reports of such attempts, it believed same and decided, consciously, to 'charge' Applicant with the allegations that it did and not with the charge that it now wants Applicant to be found guilty of. That this must be so is to a large extent borne out by the investigation it caused to be conducted. Furthermore it is clear that it must have decided not to invoke

subclause 4.1.12 of the Undertaking which reads as follows:- 'not to misuse or perform unauthorised functions on the NaTIS'. I say so given not only Respondent's failure to pertinently refer to same but also because it did in fact pertinently refer to those aspects of the Undertaking which had to be read in conjunction with the allegations that Applicant changed his passwords (twice) but failed to safeguard same. This is not the same as the situation where an employer finds an employee 'guilty' of a 'competent verdict' and a court, CCMA or bargaining Council thereafter finding that the employer was entitled, in given circumstances, to do so. Here the change (from a finding of a failure to safeguard a password at the disciplinary enquiry to one where an arbitrator is requested to make a different finding) is one to be made at the stage of the arbitration.

21. That some of the many fraudulent transactions were in fact processed by one or more employees is not in dispute. Respondent now belatedly seeks to hold all employees liable for processing fraudulent 175 transactions under their respective usernames and passwords (including Applicant whose duties do not include processing 175 transactions), this in the face of the initial decision it made in the context of the circumstances set out above. It is not for me to determine what a competent verdict is. Applicant was 'charged' with certain allegations and found guilty of same with dismissal being the result of same. In the circumstances I am of the view that I am not empowered to consider allegations relating to the intentional processing of fraudulent transactions. To now (at the stage of the arbitration) determine whether Applicant fraudulently processed the impugned transaction would result in him being prejudiced in that were he to be found guilty of same the sanction of dismissal would almost reflexively be triggered as opposed to the sanction that would be appropriate if he was found to be guilty of the allegations contained in the aforesaid charge.

22. However even if I am wrong, for the reasons set out hereunder I am of the view that Applicant did not fraudulently process the 4 impugned transactions.

23. That these transactions are fraudulent cannot be in doubt. We have the direct evidence of Jeary that there was no documentary evidence of the two relevant vehicles, i.e. the Nissan and Honda, having been tested (as there ought to have been had they in fact been tested by Jeary) at the PMB Roadworthy Centre (by Jeary or any other person). I accept that PMB Roadworthy Centre, being a grade B test station could not have issued a CRW in respect of the Nissan heavy motor vehicle (tipper). It is unlikely that a test station without the authority to issue a CRW in respect of a heavy motor vehicle would have done so given that it would be acting unlawfully and this would have been detected. Issuing such a certificate would necessarily result in it acting unlawfully if it had no authority to issue a CRW in respect of a heavy motor vehicle. Furthermore none of the owners of these vehicles questioned the deregistration of same, as one would have expected, had there been nothing questionable in respect of their registration on 24th August 2007. Given the foregoing, the absence of a CRWs in respect of same on the mgx system as well as hardcopies at the storage warehouse can only be a result of the 175 transactions in respect of them having been fraudulently processed.

24. The parties agreed that only two transactions would be dealt with given that whatever the finding was in respect of same would be equally applicable to the remaining two transactions which were processed under Applicant's username and password. I therefore find that the 4 (four) impugned transactions were in fact fraudulent.

25. All 175 transactions processed during 2007 were investigated. Of the transactions attributed to Applicant 2 (two) were processed on 24th August 2007, one on 06th September 2007 and the other on 17th September 2007, i.e over a period of 25 (twenty five) days. The passwords that were used in the foregoing

transactions were acquired by Applicant on 03rd August 2007 and 12th September 2007. It is not in dispute that at the end of 2007 or early 2008 Wagner was advised of the intention of one of the clerks, i.e. Memela (who processed 175 transactions), to steal the password of a supervisor, i.e Davenport. This in turn caused the investigation which uncovered fraudulent 175 transactions being processed during 2007 by 7 (seven) employees of Respondent, including the four transactions allegedly processed by Applicant. One such employee processed approximately 200 (two hundred) fraudulent transactions. It is not in dispute that Applicant, when supervising clerks, had to assist them in resolving problematic issues including those relating to 175 transactions. Not in dispute also is that when so assisting clerks he did so at their workstations with them standing next to him when he logged into the ENaTIS system using his personal password. Applicant's case is that this is when a clerk/s could have obtained his password which was then used to process the 4 (four) impugned transactions. If Applicant was engaged in processing fraudulent transactions he would either have been doing so to assist some other person/s or for personal gain or both. If this is so it must be improbable that such conduct occurred over a period of 25 (twenty five) days only during an entire period of approximately 365 (three hundred and sixty five) days. The period of 25 days is indicative of and points to some person/s having surreptitiously acquired the 2 (two) passwords referred to above and having utilised same to process the four impugned transactions. Had Applicant the propensity and will to process the four impugned transactions personally I would have expected him to have processed other transactions over a much longer period. I do not believe that the fact that he was at work when these transactions were processed adds much value to Respondent's case given that anyone in possession of his password could have watched his movements and processed same when it was opportune to do so. In this regard it must be remembered that two transactions were processed on 24th August 2007 and one transaction each on 06th and 17th September 2007. Neither does the fact that one transaction was processed at his workstation take Respondent's case any further given that if he processed these fraudulent transactions he would in all probability not have used his own workstation, username and password. This has to be seen in the context of him, at times, not logging off when attending to other queries. Furthermore if some other person had obtained his password Applicant's workstation could have been utilised to process the (single) fraudulent transaction whilst he was attending to other transactions. If it is argued that that would have been suspicious then that would have to apply to the three other impugned transactions because Applicant would have had to have been working alone at other workstations, given that he was processing fraudulent transactions. The probabilities favour the conclusion that he did not process the four impugned transactions.

26. (a) Having concluded that some other person/s processed these transactions was Applicant responsible for enabling him/she/them to do so by failing to safeguard his password? I have set out above the circumstances under which some other person/s could have obtained Applicant's password. Applicant must have been aware of the consequences of his password not being kept confidential. Notwithstanding the nature of his duties and the circumstances under which same was performed (which distinguishes him from the clerks he supervises) Applicant admits under cross-examination:

(i) That although he "tried as far as possible" to log off he could not do so due to the nature of his work, stating that he had to deal with irate customers "waiting at different areas of the office".

(ii) That he did not comply with clause 4.1.9 of the Undertaking the relevant part of which is that he left his workstation 'unsecured or unattended without logging off.'

(iii) That he was directly responsible (for the four impugned transactions) in terms of the Undertaking.

(b) It is clear that Applicant was aware of the importance of protecting the confidentiality of his password and the possible implications of not doing so. Having this appreciation and understanding I would have expected him to have required any person to stand away when he logged onto their workstations and not allow them at his side when he did so. I would also have expected him to have secured his or any other workstation, when he had to urgently attend to something else, by logging off.

27. The record of these proceedings clearly sets out the evidence relating to the issue of inconsistency. I will therefore not repeat same given what I believe to be the clear position. It is clear that all those identified as having processed fraudulent transactions (from Respondent's point of view) have been charged. Respondent's version as to the reason that the disciplinary enquiries of those persons in respect of whom Applicant contends he has been treated inconsistently, have not been finalised, is largely supported by his own witness, i.e Lil- Ruthan. While Respondent could possibly be accused of being inept in not finalising the aforesaid disciplinary enquiries it certainly cannot be accused of having one standard for Applicant and certain other employees and another for those like Memela who are still in its employ.

28. Having regard to all of the foregoing Applicant's conduct was negligent as charged thereby prejudicing the administration, discipline and /or efficiency of Respondent. Such negligence allowed the confidentiality of his password to be compromised, i.e. he failed to safeguard same. In the same vein not logging off also constitutes negligence in that same permitted the possibility of his password being used by others with improper motives. In this regard Applicant takes responsibility for the four impugned transactions. He is therefore guilty of the allegations contained in the aforementioned charge.

29. It is unlikely that Lil- Ruthan's version is a fabrication. He testified that at an appeals hearing, convened for the purpose of the appeals of Applicant and others dismissed for similar allegations, after he made oral submissions regarding material omissions in the transcript of the disciplinary enquiry of Applicant (and other members), Mrs Vicky Cunliffe, i.e. the Senior General Manager-Corporate Services who was the chairperson of the said Appeals Committee instructed Respondent to have a transcript of prepared by someone independent of Respondent. According to Lil- Ruthan it was agreed that he would thereafter be furnished with the independently prepared transcript whereafter he would submit supplementary submissions in respect of the said appeals. According to him the Appeal committee would thereafter reconvene to deal with the appeals. In the event no transcript was prepared and nothing further was done except that Applicant's appeal was dismissed by Mrs Cunliffe. According to Lil-Ruthan, present at this meeting were 3 (three) other persons, i.e. Nzuza the Director of Labour Relations, Mrs Ngubo the head of Legal Services and Mr Stanton Andrews "an official from the Labour Relations Component of Respondent". Nzuza's evidence that the foregoing did not occur (i.e. no appeal hearing as aforementioned was convened) and her explanation for same is not convincing partly because that she goes on to testify that she could not recall "this meeting". She was then referred to pages 225 and 226 of bundle A which is a document purporting to be minutes of a meeting of the Appeal Committee and which reflects Cunliffe, Ngubo and her (Nzuza) as being present. These minutes confirm the dismissals of all employees dismissed as a result of the investigation referred to above, including Applicant. Nzuza's response was, inter alia, that "This meeting did not take place. ..." and that when she made enquiries about same she was advised that Mr Andrews had typed Mrs Cunliffe's handwritten notes. It is apposite to state that Lil- Ruthan testified that Applicant (apart from Davenport, Miya and one other person) was with him at the appeal hearing referred to. He however conceded that he was incorrect when cross-examined stating that Applicant was "indisposed" and was not present at this appeal hearing. I would have to find that Lil-Ruthan fabricated this entire version in order to reject same (even if only on the basis of probabilities) in the face of the inconsistent and other unsatisfactory evidence of Nzuza, some if not much of which is not repeated here.

Lil- Ruthan's version of events is of such a nature that the probabilities of it being fabricated are highly unlikely. In the circumstances I accept Lil-Ruthan's version. The right to appeal is not a formality. It is there to ensure that the finding and sanction of the disciplinary enquiry is not incorrect or at least not unreasonable. To agree to obtain an accurate transcript in order to fulfil the objective of the appeal and then to decide the matter without doing so must result in such conduct being procedurally unfair.

30. The essence of Applicant's misconduct is his failure to safeguard his password. The remaining allegations, apart from not complying with the provisions of the Undertaking, was a consequence of such failure. When determining the appropriate sanction to be imposed for Applicant's foregoing failure and its consequence, regard has to be had to the fact that he functioned under pressure and also to the fact that the workplace was contaminated by a person or persons who were actively seeking to steal the passwords of other employees. Given the view that I have taken of Applicant's conduct, his password had to have been stolen on at least 2 (two occasions). That Applicant was negligent is not in dispute but the aforementioned conditions under which he worked as well as the fact that one or more co-employees were actively seeking to steal passwords must reduce the seriousness of any failure as aforementioned, i.e the degree of his negligence, on his part. That he is liable for the fraudulent transactions processed (in term of the Undertaking) with his password ought not to blind one to the fact that this liability is a fiction in that he is deemed to be liable for such (impugned) transactions even though he did not process same himself. Such liability ought not to therefore be seen to be a serious transgression. This to a large degree, is supported by the nature of the allegations with which he was charged. Applicant cannot be said to have been grossly negligent. Given that Applicant had close onto 10 (ten) years of service with no previous disciplinary infractions being proved against him as well as the degree of seriousness of the blame to be attributed to him I find that the sanction of dismissal was inappropriate in that it was too harsh. As such I find Applicant's dismissal to be procedurally and substantively unfair.

31. I have no reason to find that Applicant's conduct has rendered a continued employment relationship intolerable nor that same is impracticable. Nor is there any evidence before me to find that Applicant was the cause of the considerable delay in the finalisation of this arbitration. Since the commencement of these proceedings in 2016 the greater delays as between the parties (apart from the parties hereto not being properly notified of dates of arbitration proceedings) were occasioned by the unavailability of Respondent's witnesses. I am also alive to the fact that Applicant is partly to blame for the situation he finds himself in and that although he was dismissed in February 2009 he subsequently continued working until August 2010 up to which date he was remunerated. Having regard to the foregoing it will be inequitable to reinstate Applicant from the date that he was last employed by Applicant. I am of the view that it is just and equitable that Applicant be reinstated with effect from 01st January 2016.

AWARD

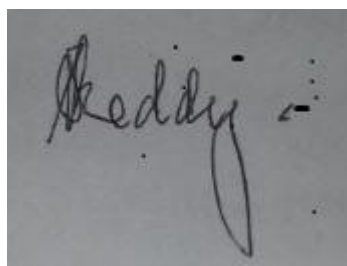
32. Applicant's dismissal is procedurally and substantively unfair.

33. Respondent is ordered to reinstate Applicant on the same terms and conditions that prevailed on 17th February 2009, within 5 days of receipt of this award.

34. The above order of reinstatement is to operate with effect from 1st January 2016.

35. Respondent is ordered to calculate all amounts due to Applicant including remuneration from 01st January 2016 to date of this award within 10 (ten) days of date of receipt of this award and to pay to Applicant, the amount so calculated, within 7 (seven) days thereafter.

36. Applicant is ordered to report for duty within 3 (three) days of receipt of this award.

A handwritten signature in black ink, appearing to read 'Reddy', is shown on a light gray background.

Part time Panellist: Sugenthran V Reddy

31 January 2021