Before the Arbiter for Financial Services

Case ASF 215/2023

AZ ('Complainant')

Vs

Bank of Valletta p.l.c.

Reg. No. C 2833

('Service Provider' or 'BOV')

Sitting of 30 May 2024

This is a complaint concerning a fraudulent payment made on behalf of the Complainant to third parties from her account held with the Service Provider.

The Arbiter is dealing with several such complaints which, while differing on certain details, contain many things in common:

1. The payment will be for an amount generally under €5,000 so that it does not get blocked for exceeding the daily limit of payments agreed between the Bank and a retail customer.

2. The fraudster manages to penetrate the means of communication normally used between the Bank and the customer, usually by SMS or e-mail.

3. The fraudster includes a link in his message and invites the customer to click on the link to make a 'validation' or 're-authentication' of his account.

4. Despite several warnings issued by the banks and the Regulator not to click on such links as Banks do not send links in their messages, and that the customer should communicate with the bank only through the official

App and/or Website through the credentials that the bank gives to customers, the customer inattentively clicks on the link.

5. Thereafter the fraudster somehow manages to penetrate the customer's account and make a transfer of money generally on a 'same day' basis that goes to the fraudster's account, usually to a bank account in Ireland or in a Baltic country from where it is almost impossible to make an effective recall of funds once the customer reports to his bank that it has been defrauded.

6. As a result, discord develops between the Bank and the customer as to who is responsible for bearing the burden of fraudulent payment. The customer claims that the Bank did not protect him when they allowed a communication channel normally used between the Bank and the customer to be penetrated by the fraudster and that the Bank should have noticed that it was a fraudulent payment because the customer generally does not have a history of such payments. The Bank maintains that the responsibility lies entirely with the customer because through gross negligence he has given the fraudster access to his account's secret credentials and thus facilitated the fraud.

In this particular Complaint, the following are the relevant details:

1. On 26 October 2023 at 10:54 hours, the Complainant received the fraudulent message on the mobile by SMS where she usually receives notifications from BOV.

2. As the Complainant felt that this was a genuine message from BOV, she clicked on the link contained in the SMS and, after a first failed attempt, she gained access to a website which she thought was that of BOV, because it seemed identical.

3. She went step by step with all the instructions given to her by the fraudster and thus entered the details to make a payment of €4,567.

4. This was done to the fraudster's bank account in Ireland and the fraudster had placed instructions to make the payment 'same day'.[1]

[1] Page (p) 46; 60

5. The payment included false name (Hannah Elizabeth Murphy) and address (XX Triq XXXXX X XXXX, Julians MT) of the beneficiary as well as a false reason for payment in order (thanks so much house looks amazing) to reduce the risk of the payment being blocked by the Bank's transaction monitoring systems.[2] [3]

6. Suspecting something was not right, Complainant contacted BOV some 3 hours later on same day but was informed that the payment had already been processed. Cards and Internet Banking were temporarily blocked.

7. The Bank maintains that the Funds left SWIFT network at 11:06 hours as the payment was marked same day and such payments are processed immediately on receipt. Furthermore, the Service Provider maintains that payments categorised as **immediate same day** could not be stopped once properly authorised.

8. A recall[4] was made by the BOV on same day at 14:36 shortly after the first report of Complainant at 14:06 hours. Further recall reminders were sent on 03 and 17 November 2023[5] but such recall was only successful to the extent of €63.19 received on 14 December 2023.[6]

9. The case was reported to the police for further investigation of the fraud.[7]

The Complaint[8]

The Complainant asserts that according to EU law quoted on the website of OAFS:

> *"the Bank must refund the payment without undue delay and by the end of the business day following the day on which it became aware of the*

[2] The SEPA system moves strictly according to IBAN number and so far does not link to the name and address of the beneficiary as stated in the transfer.
[3] P. 108
[4] *Ibid*.
[5] P. 103 - 110
[6] P. 112
[7] P. 14 - 15
[8] P. 1 -7 and attachments p. 9 - 35

> *problem, unless it has reasonable grounds for suspecting that you have acted fraudulently."*

She added:

> "*there is no reasonable grounds to suspect that it was not fraudulent and they said that they just proceed to do a transaction that seemed authorized although I have insisted, as I said only 3 hours after the transaction was executed (11AM to 14PM) that I did not do that transaction and that I have got a SMS that seemed to be from BOV requesting to unlock my Mobile App that had some restrictions. Such transfer was then authorised without me being aware I was authorising it and I let the bank know in good time manner for them to do not only a recall of the funds, which they declare has been unsuccessful, but to refund as it would correspond for any fraudulent transaction that has been flagged by the customer*".

As compensation, Complainant demanded refund of the payment of €4,567 (disregarding both the charges of the bank as well as the small recovery from the recall).

The Reply of the Service Provider[9]

In their reply of 16 January 2024, BOV explained that they declined Complainant's request for full refund as the Complainant was grossly negligent in disclosing her security credentials to the fraudsters which removed the security of the 2 Factor Authentication that the Bank is obliged to provide in order to protect clients' funds.

They gave a detailed time log[10] of how the fraudulent transaction was executed with what was evident authority of the Complainant. A detailed explanation and accompanied documentary evidence was submitted of the Bank's warnings to its clients to be careful of such scams.

[9] P. 41 - 47 and attachments p. 48 - 112
[10] P. 49 - 54

The Hearings

Two hearings were held on 25 March 2024[11] and 29 April 2024.[12]

The parties in the testimony and submissions maintained the position as explained in the Complaint and in BOV's reply.

The Complainant blaming the BOV for allowing the fraudster to penetrate the SMS channel which the Bank normally uses to communicate with her and for not noticing that the payment was a fraud.

She added:

> "***And the bank is insisting that I have made previous transactions like that, for the security, same process around seven times before which is fair enough because I have. But, also, you have to understand where the user receives a text message from the BOV channel that they normally use to communicate about mobile payments and you cannot choose that because it comes from BOV and it also says that with this code, you can go to the branch. You say, 'OK, it's also telling me to go to the branch'. Then it comes back to me saying 'Incorrect please try again' because I have typed something incorrectly. So, it is not negligence from my side; the scam was generally well done, you can say so***."[13]

On being cross-examined, the Complainant stated:

> "***I confirm that I received the SMS on 26 October at 10:54.***
>
> ***Asked whether the bank ever sent me before this an SMS with a link to follow it, I say, no; not that I remember, no.***
>
> ***Asked whether the bank ever asked me to access my internet banking or my mobile app to run an SMS, I say, no, but the bank also failed to communicate with me that there are this type of scams going on which the bank has admitted in the previous communication.***
>
> ***It is being said that the bank admitted this and offered me 20% for this, I say, correct.***

[11] P. 113 - 116
[12] P. 117 - 121
[13] P. 113 - 114

Asked what I did when I clicked on that link and what happened, I say that it was bov-banking.com so you may understand that any user might believe it to be genuine. It said that the app had to be reactivated to regain access to the mobile app and some codes were given to me which apparently were the amount of money to transfer. And I had to input the user that you normally use for internet banking transactions.

Asked where I inputted these codes, I say, on the website where they were giving me instructions to input them there. I do not remember any precise details what kind of transaction was approved. For me, I was just reactivating a code given by BOV.

Asked whether I remember using my BOV mobile app during this process, I say, yes, I think I had to, I had to put a signature code.

Asked whether I remember where I entered for the signature code on the app or what I saw, I say that I do not remember exactly how it went. What I do remember is that I had to put the username and a signature from the mobile app, but I don't remember how I got there precisely because it's been some months now.

Asked whether I remember putting any numbers, I say the ones that they instructed me to put that now I can tell that it was the amount to transfer. And then just the username, I believe, the signature code, which now I understand was to approve that transaction which I thought that it was approving the reactivation of the mobile payments.

Asked whether I was aware of the marketing campaigns made by the bank regarding such scams on newspapers and social media, I say that I was not communicated by the bank like any previous scams recently to these facts. I hadn't heard anything. I really don't visit much BOV channels; I do not follow social media because it is not my way of communication with the bank. It has always been either by phone or by the mobile app or maybe by internet banking which I do not use very often.

Asked whether I read the terms and conditions of internet banking which regulate the service which I subscribe to, I wish to say that we all read the terms and conditions; maybe we should learn more from that. But nobody, when assigned to this app or to a new account in a bank, believes that you are signing that should you fall for a scam, you just

> ***have to pay for it. We expect the bank to always protect our funds and that is the reason why people go to banks, otherwise, we will keep the money under the mattress.***
>
> ***I confirm that I made a police report regarding this incident as soon as I hung up my call with BOV's customer support.***
>
> ***Asked whether I did a follow up on this report or whether I received anything from the police, I say that I have as was recommended to me by Mr Grech but, basically, the police do not even remember how to follow up my case at all. They invited me to go back to the police station, which is frankly embarrassing but which, I guess, I still have to do. But, in my point of view, this is something that the bank should also do with the evidence they got from Revolut, the responses that the bank got from Revolut that obviously I did not get because I could not go to Revolut to do something about it and say, 'Please, refund my money,' as I am only a user.***"[14]

On the other hand, BOV claims that it fully complied with the law as provided by PSD 2[15] and Banking Directive 1[16] issued by the Central Bank of Malta.

BOV maintained that it had a robust payments system, fully in line with the two factor authentication provisions of PSD 2. Once payment was fully authenticated by the Complainant, there was necessarily gross negligence on her part which made her fully responsible for the consequences of the fraud she incurred.

In fact, in the cross-examination, the Complainant admitted that she had inputted the numbers given to her by the fraudster (which she had presumed to be BOV), including the amount, the last five figures of the fraudster's account and the authorisation code to allow the specific payment to be made, although she claimed that she did not realise that she was thus authorising a payment.

In answer to questions from the Arbiter, the Complainant explained:

> "***It is being said that in the twelve months before this incident, there were seven similar online payments and what I did with the instructions given by the fraudsters was exactly in line with what I did with the other***

[14] P. 114 - 115

[15] Directive (EU) 2015/2366 commonly referred to as PSD 2meant to safeguard the consumer (PSU) from having responsibility for payments which are not properly authorised.

[16] Directive 1 – THE PROVISION AND USE OF PAYMENTS SERVICES ref CBM 01/2018 which is modelled on the requisites of Directive (EU) 2015/2366.

seven transfers where I also put in the amount, the last five digits of the account number and then the authorisation code.

Asked whether this is correct, I wouldn't say it is exactly the same because you have to bear in mind that I received a text message saying that my access to the app has been restricted. You open it and it says that you can go to the branch with this code or … *(did not finish sentence).*

Being asked once I entered the app on the instructions of the fraudsters, the process was exactly similar to the other online payments which I had made before, I say that I don't think it works. It didn't relate to a normal transfer which I have done because the seven transfers that I had done were to myself. You can check the records that they were done to myself. and the amounts were to myself. I never do payments of that kind to other people. It is very, very rarely and probably last year there wasn't. So, firstly, when I am transferring, I am transferring to myself. And, secondly, I initiate the transaction; I never get links to it. So, the approach was different.

It is being said that the fraudster asked me to put a number in a panel which is called 'Amount'. Asked whether this raised any red flags, I say, no. Back then, no. I wish it had but back then, no. I did not even see that they put 'Amount' in there. I really cannot say that it was exactly the same process because last time we had a meeting, I was told that it was the same process and that I had done some transactions like this one which, in my mind, never happened. I am accepting the facts because I was introduced to them, but I do not deem both processes are the same."[17]

At the second hearing, the Bank produced as witness Mr _____ _____ who stated:

"***I have been working for the bank for over 30 years and employed within the Payments Multi-Channel Section for these last twelve years.***

I confirm that I have seen the complaint submitted by Miss AZ, including the fraudulent SMS.

[17] P. 115 - 116

Basically, the first step for anyone to access the Internet banking is that you have to know the login ID. The login ID is a six-digit number, the unique six-digit number which is used to access internet banking. Only the customer knows this six-digit number. So, for the fraudster to access the Internet banking, someone must have given the six-digit number to the fraudster. That is the first step, the first key that the fraudster needs to access the Internet banking. The second key is the Signature 1. So, someone again must have given the Signature 1 to the fraudster to have access to the internet banking.

At that stage, the fraudster can only view the accounts and the details of the transactions. He cannot perform any sort of transaction; to do that another signature – the Dynamic Linking - is needed. So, basically, we have three keys, the login ID, the Signature 1, the Signature 2 without those it is impossible for anyone to make any transaction.

Referring to the logs, (Doc. A – pages 49 – 53), the first part of the log, the first five lines clearly show that the fraudster, I assume without AZ knowing, took control of the internet banking and it started processing the first transaction. So, if you can see, that is the login ID, the Welcome page. Then the fraudster went into the third-party screen and filled in the details. At that point, someone gave him the Signature 2 and the fraudster processed the transaction.

I say that Ms AZ must have unintentionally given this information upon the instructions of the fraudster.

Referring now to the Session ID, the fifth column. As you can see all the logs have the same Session ID. So, we can exclude that the fraudster and Ms AZ logged out and logged in again. So, the session continued after the first payment was done.

The first three panels are basically for gaining access to view the balances, and then we start with payments to third parties. Then, there is the forecast. The forecast is actually the confirmation screen to sign the transaction. At that point, the confirmation screen was prompted.

On page 50, there are two panels dated 26/10/2023 11:03 and 26/10/2023 at 11:04 where there is 'Failed'. Those panels are actually the authentication, the Signature 2. Then, there is another panel dated

26/10/2023 11:06 where there is 'Success'. For a transaction to fail, the Signature 2, the authentication, must have been keyed in wrong.

To explain how Signature 2 works, I say that the first digits are based on the IBAN that is keyed in. The second one is the amount. You key in the amount on your token or on your mobile. And then a challenge token is given back. Now, if that challenge token is keyed in wrongly, it fails, and you can request another one. Those two failures were brought about by the wrong insertion of the authorisation codes. And the third attempt was successful. So, at 11:03 and 11:04 there was a failure but at 11:06 there was success.

The Signature 2 can only be generated by the person holding the token not the fraudster.

The rest of the log is what happened after the payment was authorized.

Either Ms AZ or the fraudster requested to print the transaction, the Print ID. And then, Ms AZ or the fraudster went to view the balances, most probably, the fraudster to check the balance was reduced and that the transaction has been processed.

I say that most probably the fraudster was in control of the Internet banking as well because as you can see from the subsequent logs, then, someone tried to do another transaction. (The first row on the 4th page – Payments to third parties).

Someone tried to make another transaction, and, because of the limit, it was not processed. What happens is that when you exceed the limit, the system will prompt that the limit has been exceeded and you will not be able to go through the authorisation stage process.

The Arbiter is asking me if I am referring to page 52 where there is a 'Failure" in the panel before the last.

I say, no, that is something different – 'No account has been assigned for this function' – usually it pops up, for example, if you try to make a third-party payment from a loan account. This is the prompt, 'No account has been assigned for this function'. Another example could be, which I don't think it is in this case, that the account requires your signature.

The Arbiter is of the understanding that what I am saying is that when they made the payment to third parties, although there is 'success' that

wasn't actually success in the in the sense that the payment was made. I say, no, because it is still in the creation stage.

But there is no log that a payment was made because the system prompts up the notification; it stops you at origin saying you have exceeded the limit.

Asked by the Arbiter whether you can distinguish from these logs what transactions were actually made by Ms AZ and what transactions were potentially made directly by the fraudster, I say, no. As I said before, for the transaction to be processed, one has to be in possession of or have access to the security. Without that, nothing can be processed.

Asked by the Arbiter whether two people can be connected to this system at the same time, I confirm that you can be on the Internet banking and on the mobile banking simultaneously.

Asked whether to approve the transaction itself there was the need of Ms AZ's involvement, I say that no transaction can be approved on its own. No, like I said before, knowingly or unknowingly, Ms AZ must have cooperated with the fraudster. Without that, it's impossible.

The Arbiter is asking when there were two failures with the transaction and the third one was a success where I explained that it probably is that the authorisation code was inputted incorrectly; and the fact that there were two failures does the system not issue a red light saying, 'Look, you know this failed twice. Better stop,' or you can make as many failures as you want and then when you get it right, it moves on.

I say that to get it right it is very difficult but, no, it doesn't stop you. What it does at Login ID stage is that if you give three login failures, then you're locked. This is at the Login ID stage and not at the payment stage. Once you are authenticated, that's it.

I confirm that Ms AZ had done payments of this kind before. We can show the statement where several transactions of similar nature were done by Ms AZ before.

The service provider is going to submit this statement in their note of final submissions."[18]

[18] P. 117 - 120

On being cross-examined, Mr _____ stated:

> "***The complainant is asking for more details regarding the two failures I mentioned when she is saying that it happened only once. She received a message from the fraudster saying that there was an error and to please start again. And this happened only once.***
>
> ***I say that the logs clearly show that the challenge token was entered twice incorrectly. I am not saying that he sent the complainant two messages, but what I can see from the logs is that the Login ID was entered twice incorrectly. I can only say what happened from the logs.***
>
> ***The complainant is referring to when I mentioned that there was a trial of an order transaction that was stopped because the amount was bigger, and this was after the first transfer was done.***
>
> ***I say, yes, because the complainant has a limit of €5,000 on the Internet banking. If you try to exceed that, it will stop you, it won't allow you.***
>
> ***The Arbiter is referring to the screen shots that the complainant submitted in her complaint. On page 18, there is a screen shot of the mobile with the message she received at 10:54 which shows that after some time there was a message saying, 'Incorrect please try again.'***
>
> ***The Arbiter is asking whether this message is what we are referring to that indicates that the transaction had failed.***
>
> ***Mr _____ replies that this message was not prompted from the bank. Referring also to the message which says, 'We have placed a restriction on your BOV mobile app for more information, please visit bov-banking.com or your local branch', Mr _____ says that the bank does not send messages like these. Even regarding the message saying, 'You can now continue to bank as normal' Mr _____ says that the bank never sends those types of messages."***[19]

[19] P. 120 - 121

Final submissions[20] [21]

In their final submissions, the parties basically restated their position as explained in the Complaint, the Reply and during the hearings, with the Complainant conceding that BOV were not at fault for the failure of their recall attempt.

The defendant also sought to excuse herself from having knowledge and experience of making such online payments by stating that payments were to her own external account and just one to a relative of hers. The Service Provider argued that the process for making such payments is the same as that applied for making the fraudulent payment complained of.

Reference was also made to the fact that the Malta Communications Authority (see next section) had confirmed that BOV had no means of preventing any fraudster from personifying himself like the Bank and using the SMS normally used by the Bank to give notifications to its customers.

Consultation of the Malta Communications Authority

For the Arbiter to understand the technologic intricacies on how a fraudster can personify himself like the Bank to defraud clients, he invited the BOV and Malta Communications Authority (MCA) security expert for consultation.

From the consultation meeting, it emerges that this type of fraud, technically known as *Spoofing* and *Smishing* or collectively as *Social Engineering Scams,* does not allow the Bank to take any precaution (other than effective warnings for customers to be careful) so that the fraudster cannot use this communication channel to defraud customers.

Analysis and consideration

The Arbiter is of the opinion that for the sake of transparency and consistency, to arrive at a fair decision on such complaints, it would be appropriate to publish a framework model on how to apportion the responsibility for fraud between

[20] P. 123 – 124 by Complainant
[21] P. 126 – 134 by Service Provider

the bank concerned and the defrauded customer by taking into account factors that may be particular to each case.

To this end, the Arbiter is attaching to this decision a framework model that he has published, and which will be used to reach a decision on how to apportion the consequences of fraud. The model also contains several recommendations for banks to further strengthen consumer protection against increasingly capable and creative fraudsters.

But the Arbiter feels the need to strongly emphasise that while it is true that banks do not have a means of prohibiting *spoofing/smishing* in the channels of communication they use with customers, they are not doing enough to sufficiently warn customers to be careful; not to click on links contained in these messages even though it appears to be coming from the bank concerned on the medium that the bank normally uses to send messages to customers.

It is not enough to make continuous announcements on their website. It is not enough to issue warnings on mass media or social media. The consumer is busy with daily problems, and it cannot be claimed that by making a notice on the website, in the traditional media or TV, or on the bank's Facebook page, the consumer is sufficiently informed. In serious cases of such fraud, it is necessary for banks to use direct communication with the customer by SMS or email. This aspect is one of the factors included in the framework model.

On the other hand, the Arbiter understands that the fact that the client errs by clicking on a link that he has been warned not to, as it could be fraudulent, this does not automatically fall into the category of gross negligence according to law.

The European Court of Justice (CJEU) in the case of Wind Tre and Vodafone Italia[22] makes reference that it would not be negligent in a gross grade if it happens even to an average consumer who is reasonably informed and attentive. The Arbiter sees complaints from complainants who easily fall into this category.

[22] Decision 13 September 2018 C-54/17

After all, PSD 2 makes it clear that the consumer must give his consent to the specific payment, and it is not enough that there is general consent as contained in any Terms of Business Agreement. Banks, therefore, need to have a sufficiently robust payment system so that payment is not processed unless it is specifically authorised by the customer.

Banks cannot escape responsibility if they leave holes in their systems whereby the fraudster can, without further involvement of the customer, make a specific authorisation of the payment in favour of the fraudster. This fact is also included in the model.

The model also considers any applicable particular circumstances of the case. There may be circumstances where the fraud message looks less suspicious. Circumstances where the customer is in negotiations for a bank loan or the customer is abroad and is carrying out transactions that are not customarily carried out by them, thus reducing the customer's suspicion that the message received may be fraudulent.

The model also considers whether the complainant is familiar with the bank's online payment to third-party systems by having made any similar (genuine) payment in the previous 12 months. This also helps to form an opinion on whether the monitoring of payments system which the bank is duty bound to make (as explained in the model) is effective.[23] [24]

Decision

The Arbiter shall decide as provided for in Article 19 (3)(b) by reference to what he considers to be fair and reasonable fairness in the circumstances and substantive merits of the case.

When the Arbiter applies the model proposed for this particular case, it arrives at this decision:

[23] (EU) 2018/389 of 27 November 2019 RTS supplement PSD2 EU 2015/2366 Articles 2(1) and 2(2)
[24] PSD 2 EU 2015/2366 Item 68(2).

	Percentage of claim allocated to Service Provider	**Percentage of claim allocated to Complainant**
Complainant who has shown gross negligence	0%	100%
Reduction because they received fraud message on the channel normally used by the Bank	50%	(50%)
Increase because the Complainant cooperated fully in making the complained payment	(30)%	30%
Increase because they had received a direct warning from the Bank in the last 3 months	0%	0%
Sub-total	20%	80%
Reduction to special circumstances	20%	(20%)
Reduction for absence of similar, genuine, monthly payments in the last 12 months	0%	0%
FINAL TOTAL	40%	60%

Therefore, according to the framework model, the Complainant should bear 60% of the weight and the other 40% will be borne by BOV.

The model finds that the fact that the Complainant continued to cooperate with the fraudster by completing the amount and last 5 figures in the Signatures of the App and then inserting the generated authorisation code specifically for the payment, as well as the fact that she had made several online payments in the

previous 12 months (although she states these were different as the payments where to herself, the process for making such payments was identical as if they were made to third parties), increases the Complainant's dose of negligence.

The model partially excuses the Complainant as she had not received a direct warning from BOV about these fraudulent schemes in the months before this case and thus offers her 20% compensation.

Furthermore, the Arbiter considers there are special circumstances which should be taken into consideration to shift a further 20% responsibility from the Complainant to the Bank. This relates to the fact that there were two consecutive failures in the input of the authorisation code at 11.03 and 11.04 and the payment was only authorised at the third attempt at 11.06.[25]

Two consecutive failures in a short time should have raised suspicion that something was not quite right. Leaving the payment system open until one gets it right after many consecutive failures is considered a weakness in the security set-up of the payment system which should be taken into consideration.

Thus, in terms of Article 26(3)(c)(iv) of Cap. 555 of the Laws of Malta, the Arbiter is ordering Bank of Valletta p.l.c. to pay the Complainant the sum of one thousand, seven hundred and sixty-three euros and sixty-one cents (€1,763.61) being 40% of the fraudulent payment less the recovery of €63.19.

Payment must be made within five working days of the date of the decision. Otherwise, legal interest starts to run from the expiry of the five days to the date of effective payment.

Since responsibility has been allocated between the parties, each party is to carry its own expenses.

Alfred Mifsud
Arbiter for Financial Services

[25] P. 50 and p. 120 – 2nd and 3rd para.

Right of Appeal

The Arbiter's Decision is legally binding on the parties, subject only to the right of an appeal regulated by article 27 of the Arbiter for Financial Services Act (Cap. 555) ('the Act') to the Court of Appeal (Inferior Jurisdiction), not later than twenty (20) days from the date of notification of the Decision or, in the event of a request for clarification or correction of the Decision requested in terms of article 26(4) of the Act, from the date of notification of such interpretation or clarification or correction as provided for under article 27(3) of the Act.

Any requests for clarification of the award or requests to correct any errors in computation or clerical or typographical or similar errors requested in terms of article 26(4) of the Act, are to be filed with the Arbiter, with a copy to the other party, within fifteen (15) days from notification of the Decision in terms of the said article.

In accordance with established practice, the Arbiter's Decision will be uploaded on the OAFS website on expiration of the period for appeal. Personal details of the Complainant(s) will be anonymised in terms of article 11(1)(f) of the Act.