Before the Arbiter for Financial Services

Case No. 058/2019

JO (the complainant)

vs

HSBC Bank Malta p.l.c. (C-3177)

(the service provider/the Bank)

Sitting of the 13 September 2021

The Arbiter,

Having seen the complaint whereby the complainant submits that:

He realised on the 12 December 2019 that his Visa card had been used without his knowledge or authorisation to make several €1,000 transfers to another account and, also, some purchases which totalled €5,334.98.

He was only made aware of the transactions when the person who was known to him indicated that he had stolen the money from his account.

At this point, the complainant called the Bank to cancel his Visa debit card which was not physically stolen. He immediately told the Bank's operator to immediately cancel the card. The operator confirmed that the majority of his money had already left the account.

There were still 2x€1000 transactions pending which he asked to cancel but the operator advised that he was unable to do so. He advised him to visit his local HSBC Branch the next day to fill out a disputed transactions form.

He filed the disputed transactions form that day and was told that he will hear from the Bank in the following weeks. He did not receive any feedback till the 6 February when the day before he had emailed the Bank asking for any update.

He was informed by phone by the Bank that his claim was being rejected by the Bank without offering him any valid or legal reason. Upon his request, this was confirmed by email.

The reasons for the complaint are the following:

1. That he was not contacted by the Bank to highlight unusual and suspicious activity on his card or blocking the transactions;
2. Failure of the investigating team to record and collect all relevant details of the case before making a decision to reject the claim;
3. Failure to provide answers to several questions, for example, when the 3D authentication password was created and whether it corresponded with the date of the initial fraudulent transaction;
4. Failure to provide a legal reason under the Payment Services Directive 2 (PSD 2) to reject the disputed transactions claims;
5. Failure by the bank to cancel pending transactions or even to try to contact the 'transfer firm' (Transferwise) to notify them not to cash the funds in question;
6. The Bank's lack of understanding and empathy throughout the traumatic event;
7. The Bank's bad handling of the case which he found unprofessional, frustrating, undecisive and some of their communications did not convince him of a professional handling of the case.

Remedy

The complainant is asking the Arbiter to award him the total amount of the transactions, that is, €5,334.28, and another €5,000 for the distress caused to him by the Bank by the bad handling of the case.

Having seen the reply by the Bank which states:

1. That the Complaint is unfounded and ought to be rejected because of the following reasons:

   (i) That preliminarily, the Complaint is null and void and ought to be rejected with costs because *ex admissis,* the Complainant has already filed an action in court against the Complainant in the UK. The Bank respectfully submits that the Complainant is seeking redress against the relevant third party in the UK on the basis of fraud and is also seeking redress from the Bank on the basis of unauthorised transactions – for the same amount – on the same transactions in Malta – meaning that the Claimant is seeking to benefit from double remedy.

   (ii) That preliminarily and without prejudice to the above, the Bank pleads that the Financial Services Arbiter does not have jurisdiction to determine this case as the basis of this claim is based on the notion of unjustified enrichment which is outside of the Arbiter's remit as determined by Chapter 555 of the Laws of Malta.

   (iii) That primarily and without prejudice to the above, no claim for monetary compensation owing to alleged distress suffered can be tabled before the Arbiter when such falls outside the Arbiter's competence under Chapter 555 of the Laws of Malta.

   (iv) That, without prejudice to the above:

      A. The first and fifth allegations which are the Bank's failure of '*not contacting the Complainant to highlight the unusual and suspicious activity on his card or blocking the transaction in question*' and failure to '*cancel the pending transactions or to even try and contact the transfer firm in question (transferwise) to notify them to not cash out the funds in question*' are unfounded and based on an improper understanding of the manner in which electronic transfers occur.

      Primarily, it is to be noted a priori that the transfers that were affected and which the Complainant seeks refund thereof were

carried out via the 3D secure system which is subject to client authentication, ensuring the authenticity of both peers, the server and the client, using digital certificates.

The Bank is sure that the Arbiter is aware that the real time element in electronic transfers is crucial. If every merchant or every payer could not rely on the real-time assumption and had to wait until the bank's employees were about to go home at the close of the banking day before he could with confidence rely on the transfer having been made so as to enable the payer to complete a purchase, it would be necessary for conveyancing to return to the system of physical completion which, in today's world, is inconceivable. In fact, the use of the 3D Secure system, and thus the entry of password authentication to access and peruse such system, does not, as a rule, envisage the possibility of chargeback rights as this will distort and undermine the element of security that is the prevailing scope behind the 3D Secure system.

Based on the above and in the context of the allegation being made, the Bank notes that, nevertheless, the request for the revocation or cancellation of the transfers by the Claimant did not reach the Bank in due time because the transfer had already taken effect and the Bank could no longer cancel the payment instruction or nullify it by a counter-instruction. Also, in this case, the request for revocation was too late as the instruction was fully performed by the Bank's **automated system.**

The transmission of data on the transfer form in the computer marks the decisive moment, because at this time the bank has done all that is necessary to bring about a credit entry in favour of the transferee. From this moment it can no longer interfere with the entering procedure.[1] Electronic fund transfers are never any more than the automated exchange of messages from

[1] Draft Legal Guide on Electronic Funds Transfers of the United Nations Commission on International Trade Law, as to when funds transfers become final: United Nations, General Assembly, A/CN, 9/266/Add. 1 of 30 April 1985.

the client to the bank, between different banks and then from the bank to the transferee. This exchange of messages finally results in a set of written messages to debit or credit the respective accounts. No funds are exchanged as such, the procedure simply involves variations in the debits and credits to the accounts concerned, which can be carried out more quickly due to the use of automated techniques.

To argue that the transfer is the result of simply of the actions of the Bank officials is analogous to arguing that a cheque is not efficacious to recognition of a debt which is due because there has to be a bank activity before a credit appears in the payee's account. In either case, the activity at the bank is simply the incidental machinery by which the document is given its practical and intended effect, just as the postman who delivers the envelope containing a cheque becomes part of that incidental machinery.[2]

If a person obtains a cheque book by false pretences and uses it to buy goods, then that person is guilty of an offence but the bank cannot be at fault should the merchant provide a validly executed cheque which has been signed and validated and consequently deducts funds from the payer's account.

The basic effect of these automated techniques is a dematerialisation of the operations, that is to say the total or partial disappearance of the written paper which is signed at the time of issuing and the disappearance of the bank employee waiting to transmit and execute a payment order who is replaced by electronic pulses which can be processed directly by computer.

Triggers within the Bank's internal system are in place to alert the attention of the bank in the event of a transaction which is of an obviously unusual nature (for example the amounts are higher than normal). In electronic transfers checks based on a

[2] This was also confirmed in R v King [1992] Crim. L.R.47; [1991] 7 WLUK 5 (CA)

personal element of the transferor using passwords and Personal Identification Numbers or CVV numbers do exist so the Bank's security system has a commercially reasonable method of security which includes the insertion of login names, passwords, PIN numbers and secure key coding which are all techniques for controlling access and identifying users. In this case, the Complainant was identified, and the electronic transfer was affected. The Complainant has allowed his card details to be accessed even though it has now been repeated *ad nauseum* by the Bank (via its website, terms and conditions, marketing campaigns, etc.) that account holders are never to share their bank or personal information with anyone and one is to immediately (not 6 days later) contact the bank should an account holder suspect that his data has been accessed. This is resultant from Paragraph 9 of the relative Terms and Conditions, herewith attached.

B. With regards to the second allegation, the onus is on the Complainant to prove that the Bank did not investigate the matter. To the contrary, the Bank has conducted the necessary internal investigation as shall be evidenced in the course of these proceedings.

C. With regards to the third allegation and the 3D Secure authentication, once again it is evident that the Claimant fails to understand a number of concepts relevant to electronic transfers.

   The Bank respectfully submits that according to the police report submitted by the Complainant, the Complainant was 'robbed' on the 7 December 2018, yet he only decided to inform the Bank of the 'possibility' that his cards were stolen on the 13 of December 2018 – 6 days later.

   It is a known fact that cashless transfers and electronic techniques increase the speed with which transfers of funds can be made. It is clear that a higher degree of diligence on the part

of the parties involved is required. Indeed the customer (in this case, the Complainant) has to react promptly when he identifies an anomaly either by reading the statements of account available online at any time on a regular basis or by notice from his contracting party (in this case, the Bank). In cashless transfers which are done using 3D secure (that is the name, identity card number, login PIN, password and secure key are entered prior to a transaction), the account holder bears the entire risk of any transactions carried out following the loss or misuse of credit cards, up to the time at which he notifies the bank of the illegal transactions and up to the time the bank is able to take adequate measures to prevent any further transactions. Also, in terms of Article 71 of PSD II a payment service user is to inform the Bank 'without undue delay' on becoming aware of any unauthorised transaction.

Given the disappearance of the personal elements (such as signature and so on) which can be used to authenticate the transfer order, the financial institutions take care to specify that data records constitute an admissible or even restricting element of proof if the origin, amount or recipient of the order is disputed. This is clearly designed to render the customer responsible for fraudulent orders transmitted using his means of access.

The 3D Secure system which the bank has implemented is a reliable system which ensures that the person issuing the order is indeed the authorised transferor. It is reliable to the extent that the transmission of a fraudulent order is not due to failure of the security system but rather to a negligent act by the customer who has not observed the security instructions (such as not disclosing the PIN number to a third party). The Bank did have this system in place and confirms that the transfers were carried out using 3D Secure.

D. With regards to the fourth allegation that the Bank failed to provide an '*eligible legal reason under the PSD II to reject the*

disputed transaction', the Bank respectfully asks the Arbiter to refer to Letter 1 and Letter 2, sent to the customer the content of which clearly include clear, eligible, reasons for the Bank's refusal. It would seem that even though the reasons are as clear as day, the Complainant fails to read them since they are not the reasons he is expecting to read.

Letter 1 dated 26 February 2019, paragraph 4:

'*Please note that in line with our terms and conditions, if a Card is lost or stolen or liable to be misused you are required to notify the Bank immediately. We confirm that the disputed transactions were ALL completed before the Bank was informed to stop the card and it was therefore not in a position to take any action to stop the card or the transactions until after these had taken place.*

On the above basis, please note that your request for a refund on the relevant amounts is not justified in the Bank's regard and is being declined.'

Letter 2 dated 13 March 2019, paragraph 5:

'*Irrespective of the changes you made to the Police Report the fact remains that you should have been aware on the 7 of December 2018 that your cards had been compromised and you should have reported same to the Bank immediately.'*

E. That with regards to the sixth allegation and seventh allegation, the Bank entirely refutes the allegation that the Bank acted unprofessionally, or without empathy. The Bank did contact the Complainant on a number of occasions and discussed the matter in detail with the Complainant, but the Complainant was not content with the Bank's reply and these allegations of lack of empathy ensued. The Bank has always acted in accordance with the standards required by the regulatory framework and in accordance with the highest standard of diligence under

applicable law and, if need be, this could be adequately proved during the hearing of this case.

F. That, without prejudice to the above, the Bank cannot be found liable or responsible for the unjustified enrichment of a third party and neither can it be at fault for allowing the authorised transaction to proceed.

It shall be evidenced that the log (computer generated list of transactions carried out by the Bank) constitutes formal and satisfactory proof of the orders issued by the subscriber. The system operates as follows. The log generated by the bank's computer is deemed to register the customer's instructions faithfully. This means that the customer is liable for the order issued from his premises or using his PIN code until it reaches the bank's computer. It is not possible at law to deceive a machine. In the modern world, where internet banking involves the transfer of funds by the use of passwords (as in the present case), it is regrettable that obtaining by means of PIN numbers, passwords and the like operating on computers by a person who knows that he has no right to do so is not a substantive offence of unauthorised transactions against the Bank but an offence against computer misuse.

G. That *ex admissis,* the Complainant informed the Bank that his personal details (which would have included his personal security verification details) were left in his wallet (*vide* email dated 7 February 2019 attached to Complainant's Complaint Form) which wallet was found by third parties house guests of the Complainant. This would amount to gross negligence in terms of PSD II on the basis that the Complainant had allowed the house guest access to his details without any difficulty whatsoever.

H. With regards to the fact that the Bank did not inform him of the transaction, the Bank notes that the Complainant had not signed up for the service by means of which the Bank would transmit

SMS alerts to his mobile phone. This service may be easily signed up to via the Bank's general banking portal. The Complainant cannot complain of lack of a service he had not signed up for.

I. That the Bank entirely refuses the allegation that the Bank acted unprofessionally, or without empathy. The Bank has always acted in accordance with the standards required by the regulatory framework and in accordance with the highest standard of diligence under applicable law and, if need be, this could be adequately proved during the hearing of this case.

2. That in view of the above, it is submitted that there could be no remedy to the Complaint as the Complaint is unfounded in fact and at law.

3. The Bank respectfully reserves the right to produce further oral and documentary proof and to make additional submissions both oral and also in writing during the sittings before His Honour, the Arbiter, to substantiate its position as above indicated.

4. For the above reasons, the Bank humbly submits that all Complainant's demands are to be rejected with costs to be borne by said Complainant.

Having heard the parties and seen all the documents

Considers

The Arbiter shall decide the case by reference to what in his opinion is just, equitable and reasonable in the particular circumstances and substantial merits of the case.[3]

Preliminary Pleas

Action before another Court

The service provider submitted that the complaint is null and void because the complainant has already filed an action in court against '*the Complainant in the UK'*. As written this plea does not make sense because it states that the

[3] CAP. 15 of the Laws of Malta, Art. 19(3)(b)

Complainant has filed an action in the UK against himself. From the records of the case this does not result. The complainant has only stated that he reported his former partner to the UK police for stealing the card information from his wallet. This is not the subject matter of this case.

Article 21(2)(a) of Chapter 555 of the Laws of Malta stipulates that:

'An Arbiter shall decline to exercise his powers under this Act where:

(a) the conduct complained of is or has been the subject of a lawsuit before a court or tribunal or is or has been the subject of a complaint lodged with an ADR entity in any other jurisdiction, initiated by the same complainant on the same subject matter'.

The service provider did not prove that the '*conduct complained of by the complainant has been the subject of a lawsuit before a court or tribunal'* or another ADR entity. Therefore, this plea is being rejected.

The second plea is to the effect that the service provider is contending that this case is a case of unjustified enrichment and, therefore, falls outside the jurisdiction of the Arbiter.

Apart from the fact that Chapter 555 of the Laws of Malta does not preclude the Arbiter from considering such pretences, the nature of this case is not a case of unjustified enrichment, but the complaint is about the conduct of a service provider in relation to his client to whom the Bank has offered its services.

As agreed by the parties even in their submissions, the case falls *inter alia* within the parameters of **Directive 1 of the Central Bank of Malta** (**the Directive**) and the **Payments Services Directive 2 (PSD2).** Therefore, this plea is being rejected.

Plea number three regarding any compensation that may be awarded to the complainant, will be dealt with by the Arbiter when he deals with the merits of the case.

The Arbiter would like to underscore that Chapter 555 of the Laws of Malta[4] emphasises that the main scope of these proceedings is the conclusion of the dispute on its own merits rather than the sporting of a legalistic exercise which

[4] Specifically, Article 19 (3)(b)

very often beats the purpose of an ADR entity which should not be considered as another Civil Court. Therefore, the Arbiter appreciates that unnecessary preliminary pleas should not be raised because they are a time-wasting exercise for the Arbiter.

The Merits of the Case

The complainant is basically claiming that the Bank should indemnify him the sum of €5,334.28 being the amount of '**unauthorised transactions'** carried out by his former partner who stole information from him relating to his debit card. The complainant is also asking for another €5,000 for the alleged distress caused to him by the Bank in the bad handling of the case.

On its part, the service provider submits that it should not disburse these amounts because, firstly, the Bank carried out its obligations according to law and specifically it observed its duties under the Directive and PSD2.

Card Theft/Fraud

The complainant submitted that on the 7 December 2018, an ex-partner had access to his card details and made unauthorised transactions and stole money from his account

Card fraud/theft has been defined as:

'*a form of identity theft in which an individual uses someone else's credit card information to charge purchases, or to withdraw funds from the account. Credit card fraud also includes the fraudulent use of a debit card, and may be accomplished by the theft of the actual card, or by illegally obtaining the cardholder's account and personal information, including the card number, the card's security number, and the cardholder's name and address.'*[5]

Card theft/fraud materialises when the card or card details or security codes are obtained without the cardholder's consent and used to make '*unauthorised*' transactions for the abuser's benefit or for the benefit of another person.

The dispute normally arises when the service provider refuses to refund the cardholder for the amount stolen from his account. Basically, this is what this

[5] https://calert.info/details.php?id=1669 - CASE STUDY: DEBIT AND CREDIT CARD FRAUD
24 March 2018 Bachir El Nakib (CAMS), Senior Consultant Compliance Alert LLC

case is all about. Although banks insist that they should not pay for fraud, these unfortunate situations are regulated by the Payments Services Directive 2 (PSD2) as transposed in our law by Directive 1 of the Central Bank of Malta (the Directive)

Legal Aspects

The unauthorised access to the complainant's card by his ex-partner took place on the 7 December 2018. By that date, the ***PSD 2*** and the Directive were **already in force.**[6]

The Directive *inter alia* delineates the rights and obligations of the *payer/payment user* and also those of the service provider.

The Arbiter will make reference only to those parts of the Directive/PSD2 which are relevant to the merits of this case.

The payer/user is *inter alia* obliged:

45. (1) The payment service user entitled to use a payment instrument shall:

(a) use the payment instrument in accordance with the terms governing the issue and use of the payment instrument, which must be objective, non-discriminatory and proportionate;

(b) notify the payment service provider(s), or the entity specified by the latter, without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument;

(2) For the purposes of Paragraph 45(1)(a), the payment service user shall, in particular, upon receipt of a payment instrument, take all reasonable steps to keep its personalised security credentials safe'.

On the other hand, the payments services provider has *inter alia* the following obligations:

46. (1) The payment service provider issuing a payment instrument shall:

(a) make sure that the personalised security credentials are not accessible to parties other than the payment service user that is entitled to use the payment

[6] Directive 1 came into force on the 13 January 2018

instrument, without prejudice to the obligations on the payment service user set out in Paragraph 45;

(b) refrain from sending an unsolicited payment instrument, except where a payment instrument already given to the payment service user is to be replaced;

(c) ensure that appropriate means are available at all times to enable the payment service user to make a notification pursuant to Paragraph 45(1)(b) or to request unblocking of the payment instrument pursuant to Paragraph 44(4);

(d) on request, the payment service provider shall provide the payment service user with the means to prove, for 18 months after notification, that the payment service user made a notification as referred to in Paragraph 46(1)(c);

(e) provide the payment service user with an option to make a notification pursuant to Paragraph 45(1)(b) free of charge and to charge, if at all, only replacement costs directly attributed to the payment instrument;

(f) prevent all use of the payment instrument once notification pursuant to Paragraph 45(1)(b) has been made.

(2) The payment service provider shall bear the risk of sending a payment instrument or any personalised security credentials relating to it to the payment service user.

Reimbursement

According to Article 49(1) of the Directive, in the case of an **unauthorised** transaction, the bank is obliged to '*refund the payer the amount of the unauthorised payment transaction immediately'* unless the bank has proof that the card user had acted fraudulently.

There is no definition either in the Directive or in the Card Conditions of Use of what is an authorised transaction. However, it has been widely held that for a transaction to be authorised there must be the consent of the card user for that transaction.

For instance, the UK Ombudsman for Financial Services in its notes explain that:

'*One of the important questions to consider is whether the payment in question is authorised. In broad terms, "authorised" in this context means that a consumer gave their bank an instruction to make a payment from their account, in line with its terms and conditions**. In other words, they knew that money was leaving their account – wherever that money actually went**.'*[7]

The Arbiter fully agrees with the requisite of *'knowledge'* of the transaction by the payment services user because there can never be consent or authorisation unless the user knows about the transaction.

Service providers are also aware that certain transactions may not be authorised by the card user and provide rules and conditions in this respect. For instance, in the Conditions of Use established by the service provider in this case, on page 6 of the Conditions under heading 9, the service provider established the procedure to be used by the cardholder in the eventuality of '*loss, theft or misuse of the card*'.[8]

The Directive basically states that if a cardholder has not authorised a payment, the bank should refund the money.

However, this is not a *carte blanche* to the cardholder and there are certain limitations.

For instance, Article 50 of the same Directive stipulates that:

'*the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument. '*

However, this does not apply if:

'(a) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, except where the payer has acted fraudulently.'

The payer will not be entitled to a refund if the transactions

[77] https://www.financial-ombudsman.org.uk/businesses/complaints-deal/fraud-scams
[8] Pg. 76

'*were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Paragraph 45 with intent or gross negligence.*'[9]

Therefore, the Arbiter has to consider whether the complainant has acted **fraudulently** or failed to observe the conditions of use of the card[10] '***with intent or gross negligence'*.**

There is no proof that the complainant in any way acted fraudulently. The doubt expressed by the service provider that there could have been collusion between the complainant and his ex-partner is not backed by any solid proof and, therefore, the Arbiter cannot entertain such doubt. The complainant clearly explained that had there been collusion with his ex-partner it would not have made sense for him to report him to the police or Action Fraud as he actually did. Therefore, the Arbiter is justified in excluding any fraudulent behaviour by the complainant.

However, the Arbiter must also consider whether the complainant is responsible for **gross negligence**. Both PSD2 and the Directive do not define what constitutes gross negligence.

The concept of gross negligence seems to differ between common law countries, like the UK, and other jurisdictions, that apply civil law. In the UK, gross negligence is very often regarded as negligence on a higher degree than mere negligence.

On the other hand, the Maltese Courts have considered gross negligence as based on the Roman Law concept of *culpa lata* (*grave fault*) where there is an element of *dolo (intentional tort).*

The first case decided by the Arbiter regarding the fraudulent use of a credit card was decided when PSD 1 was still in force. Although both PSD1 and PSD2 do not define gross negligence, in *recital*[11] 72 of PSD2 there is an explanation and an illustration on what might constitute *gross negligence*:

[9] Art. 50(1)(a) of the Directive
[10] According to Art. 45
[11] Preambles preceding the dispositive parts of a Directive can either be Citations or Recitals. The scope behind recitals is to '*set out the reasons for the contents of the enacting terms (i.e. the articles) of an act.* http://publications.europa.eu/code/en/en-120200.htm

'In order to assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, ***keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties.***[12] *Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer should be considered to be null and void …'.*

There is controversy on the legal binding force of recitals.

However, the European Court has held that a recital does not have a legal binding force:

'*the preamble to a Community act has no binding legal force and cannot be relied on as a ground for derogating from the actual provisions of the act in question.'*[13]

However, preambles can be relied on for interpretation purpose:

'*Recitals can help to explain the purpose and intent behind a normative instrument. They can also be taken into account to resolve ambiguities in the legislative provisions to which they relate'.*[14]

Moreover:

'*Recitals can help to establish the purpose of a provision*[15] *or its scope'.*[16]

[12] Emphasis by the Arbiter

[13] Case C-162/97, Nilsson, [1998] ECR I-7477, para. 54. As quoted in 19TH QUALITY OF LEGISLATION SEMINAR 'EU Legislative Drafting: Views from those applying EU law in the Member States' EUROPEAN COMMISSION SERVICE JURIDIQUE - QUALITY OF LEGISLATION TEAM Brussels, 3 July 2014, *Complexity of EU law in the domestic implementing process.*

[14] Case C-244/95, Moskof, [1997] ECR I-6441, paras. 44-45, As quoted in footnote 10

[15] Case C-173/99 BECTU [2001] ECR I-4881, paras 37-39), op.cit

[16] (Case C-435/06, C [2007] ECR I-10141, paras. 51-52), op.cit

In this context, the Arbiter considers that the recital 72 of PSD2 can be helpful in trying to understand what the European legislator had in mind in relation to Article 50 of the Directive which reflects the relevant provision in the PSD2 text.

The recital basically explains that:

1. In order to assess possible negligence or gross negligence on the part of the complainant account should be taken of all of the circumstances;
2. the concept of negligence implies a breach of a duty of care; **gross negligence should mean more than mere negligence;**
3. keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties is a form of gross negligence.

The Circumstances of this case

The Arbiter has to look carefully at the circumstances behind the complaint, examine the evidence and decide – on a balance of probability what he thinks has happened and who should fairly and reasonably bear the loss.

The complainant explained that:

'*On 7 December 2018, an ex-partner of mine gained access to my property without my knowing, the card details were taken down. I do not know exactly how they were taken as the card was not physically taken.'*

However, when he originally made the report to the police, he stated that his property had been broken into and his cards and the details were stolen:

'I am being questioned why in my police report I stated that my property was broken into and my cards were stolen, and then I changed the version and then said to the bank that my property was broken into but my cards were still in my possession, I reply that in the initial statement to the police I just said the card was stolen but, actually, the card was not stolen; the details of the card were stolen. At that time, I was in a panic and it was rather very quick. That was not

the case though, it wasn't the physical card that was stolen but the details of the card were stolen*. The card was in my wallet; it had not moved from the wallet'.*[17]

Moreover, he does not give an explanation how his partner might have had all the details about his card and the security features of the card.

However, he stated that his partner used to live with him and had access to his wallet:

'*My ex-partner is identified as Mr Scott Macdonald. This person has benefitted from my debit card. He had access to my property and lived in my property. A police report was filed against Mr Scott Macdonald personally. Reference is made to an email I sent to the bank, where I said that he had easy access to my information, to my wallet and to the information in my wallet, and I say, yes he would have access to it as he was living with me. My I.D. card would have been in the same wallet.'*[18]

He did not give a tangible explanation how his ex-partner used the 3D password. He says that he had not written it down anywhere and he knew it from memory.

Moreover, the complainant is also inconsistent on the use of his card. Being questioned whether he used the card for online gaming, where he had spent €6,000 on a gaming site, he said that he had used a different card. When confronted by the Bank that, in fact, he had used the same card merits of this case, he evaded the question by saying that the PIN was not written anywhere.

Asked whether his ex-partner and himself ever made transactions together online, he did not deny but simply said: '*I reply that I have no recollection of doing so'.*[19]

He also admits that his ex-partner had '*easy access to my wallet and to the information in it'.*[20]

[17] Pg. 91
[18] *Ibid.*
[19] Pg. 92
[20] *Ibid.*

The Bank stated that the transfers that were effected were carried out via the 3D Secure system which is subject to client authentication '*ensuring the authenticity of both peers, the server and the client, using digital certificates'*.[21]

From the facts emerging from this case, the Arbiter can only come to the reasonable conclusion that, unfortunately, the complainant had allowed his card details and the security features easily accessible to third parties, in this case, to his ex-partner. He admitted that his ex-partner had easy access to his wallet and to his card and did not exclude that his ex-partner and himself had made online transactions together.

The *Card Conditions of Use* clearly state that upon receipt of the PIN, the notification should be destroyed and the PIN number memorised and not be accessible to anyone. Moreover, the cardholder should '*take all reasonable precautions to prevent the card and PIN from being used fraudulently'*.[22]

Moreover, the example given in PSD2 recital of what constitutes gross negligence tallies with the facts of this case. It is the Arbiter's considered opinion that the complainant allowed easy access of sensitive card information to his partner who abused of the situation and defrauded the complainant.

Conclusion

Considering all the facts of the case, the Arbiter does not consider the complaint to be fair, equitable and reasonable and cannot uphold it.

Since the Arbiter has rejected the preliminary pleas raised by the service provider, each party is to bear its own costs of these proceedings.

Dr Reno Borg
Arbiter for Financial Services

[21] Pg. 52
[22] Pg. 76