An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

Decision Ref:	2018-0198
Sector:	Banking
Product / Service:	Current Account
Conduct(s) complained of:	Disputed transactions
Outcome:	Rejected

LEGALLY BINDING DECISION OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

Background

This complaint relates to unauthorised transactions on the Complainant's current account held with the Provider.

The complaint is that the Provider wrongfully failed to reimburse the Complainant for the disputed transactions on her current account.

The Complainant's Case

The Complainant submits that on 14 December 2016 she received a text message at 2.24am from the Provider's Debit Card Security to verify three transactions that had occurred since midnight. The Complainant submits that she replied "no" to confirm that she had not carried out these transactions, and received another text message to advise that a Card Security Agent would be in touch as soon as possible.

The Complainant submits that at 4.04am she received another text message providing a number to telephone, which she did. The Complainant submits that the Provider's representative asked her did she have her debit card or did she provide her debit card details to anyone via telephone or email. The Complainant states that "*Thinking about it I realised that I had received an email on the 13th as I thought from [the Provider] to update my account or I would no longer be able to access it from the 15th Dec. This I'm afraid I did respond to*".

The Complainant submits that the Provider's representative gave her another number to telephone in the morning to fill out a phishing form. The Complainant states, "*I was given*

the impression that I was lucky they had found out in time and to leave it with them, and their Fraud Investigation unit". The Complainant also states that "*As the [Provider's] Card Security Agent was notified that these were not my transactions on the 14/12/16 I can't understand why the monies were debited out of my account on the 16/12/16. The three transactions in question amount to €793.70*".

The Complainant is seeking for her current account to be credited by the amount fraudulently taken from her account.

The Provider's Case

The Provider submits that the Complainant advised, during her conversation with its card security Department on 14 December 2016, that she received an email purporting to be from its online banking Department. The Provider submits that the Complainant stated that she clicked the link in this email and entered in her details and information, as she believed this was a genuine email. The Provider submits that as a result of the Complainant divulging this information to a third party, a 3D Secure password was set up and used to carry out these transactions.

The Provider states that "*3D Secure has been set up as an added security on [named] Debit Cards and guards against unauthorised use online. Like the PIN, it should only be known to the person to whom the card is issued. The 3D Secure feature is embedded into the use of the [named] Debit Card with certain retailers: therefore, it is necessary to register for the 3D Secure feature, if you wish to shop online with these retailers*".

The Provider submits that on 20 December 2016 its Fraud Investigations Team sent the Complainant a letter confirming that she would remain liable for the disputed transactions as she was in breach of the terms and conditions of her account.

The Provider submits that it cannot refund the sum of €793.70 to the Complainant as she is in breach of her terms and conditions.

Decision

During the investigation of this complaint by this Office, the Provider was requested to supply its written response to the complaint and to supply all relevant documents and information. The Provider responded in writing to the complaint and supplied a number of items in evidence. The Complainant was given the opportunity to see the Provider's response and the evidence supplied by the Provider. A full exchange of documentation and evidence took place between the parties.

In arriving at my Legally Binding Decision I have carefully considered the evidence and submissions put forward by the parties to the complaint.

Having reviewed and considered the submissions made by the parties to this complaint, I am satisfied that the submissions and evidence furnished did not disclose a conflict of fact such as would require the holding of an Oral Hearing to resolve any such conflict. I am also

/Cont'd…

satisfied that the submissions and evidence furnished were sufficient to enable a Legally Binding Decision to be made in this complaint without the necessity for holding an Oral Hearing.

A Preliminary Decision was issued to the parties on 5 November 2018, outlining the preliminary determination of this office in relation to the complaint. The parties were advised on that date, that certain limited submissions could then be made within a period of 15 working days, and in the absence of such submissions from either or both of the parties, within that period, a Legally Binding Decision would be issued to the parties, on the same terms as the Preliminary Decision, in order to conclude the matter.

In the absence of additional submissions from the parties, the final determination of this office is set out below.

The issue to be determined is whether the Provider wrongfully failed to reimburse the Complainant for the disputed transactions on her current account.

The Complainant submits that the Provider was aware that the transactions were not hers, however it still paid out the money. The Complainant states that the Provider *"knowingly debited my account two days after I [notified it] that those transactions were not mine*". The Complainant submits that the Provider's investigation team did not follow up on where or to whom the goods were sent. The Complainant states that "*I have been onto my local Gardaí and they too asked me did [the Provider] not follow up on where the purchases went to?*"

The Provider submits that the following transactions debited the Complainant's account amounting to €793.70:

Date	***Merchant***	***Amount***
14/12/2016	*M and M Direct Ltd*	*€140.08*
14/12/2016	*M and M Direct Ltd*	*€23.93*
14/12/2016	*NEXT DIRECTORY*	*€629.96*

The Provider has submitted a copy of the transaction history on the Complainant's current account, and I note that these transactions were carried out at 2:09am, 2:12am and 1:59am respectively.

The Provider submits that these transactions were made prior to the misuse of the Debit Card being reported to it, and were completed using a combination of the valid card details together with a valid 3D Secure password. The Provider states that "*3D Secure works by using a password that is created as a unique online identifier. This is then used to validate online transactions with participating online retailers. The information supplied is not passed to the online retailer. Since the card is protected by a 3D… Secure Password, only persons with the password, or in possession of specific personal information that was used to set up the password can use the card online*".

/Cont'd…

The Provider submits that to set up a 3D secure password the following information is required:

- Card Number
- CVV (three digits on the back of the card)
- Name on Card
- Date of Birth
- First/last four digits of the bank account number

The Provider submits that it received an authorisation request for the disputed transactions on 14 December 2016. The Provider submits that it approved the authorisation as the transactions were completed using a 3D Secure Password and the Debit Card details were used to carry out the transactions and it was not on notice of any wrongdoing. The Provider submits that it was obliged to honour the transactions as the security measures had been fulfilled and it was not in a position to cancel the approved authorisations. The Provider states that it is "*not obliged under the Terms and Conditions of the Use of the [named] Debit Card to monitor the Complainant's transactions on her account*".

The Provider has obligations pursuant to the European Communities (Payment Services) Regulations 2009 (hereinafter referred to as the "2009 Regulations"). The 2009 Regulations implement a set of rights and obligations where a consumer engages a Payment Service Provider, such as the Provider in this case, to carry out a Payment Service by means of a Payment Instrument and/or a set of procedures. The Regulations set out how a transaction using a card can be carried out with consent by the accountholder and also how such a transaction is classed as authorised or unauthorised. Specifically, Regulation 68 of the 2009 Regulations states that:

> *68. (1) A payment transaction is authorised only* ***if the payer concerned has consented to its execution.*** *A payer can authorise a payment transaction before or, if agreed between the payer and the payment service provider concerned, after the execution of the payment transaction.*
>
> *(2) Consent to execute a payment transaction or a series of payment transactions is valid only if given in a form agreed between the payer and payment service provider concerned.*
>
> *(3)* ***In the absence of consent, a payment transaction is unauthorised.*** (my emphasis)
>
> *(4) A payer may withdraw his or her consent at any time before the time of irrevocability under Regulation 82. A payer may withdraw his or her consent to execute a series of payment transactions with the effect that any future payment transaction is unauthorised.*
>
> *(5) The procedure for giving consent shall be as agreed between the payer and the payment service provider."*

/Cont'd…

The Provider submits that the mechanism for indicating consent to the transaction on the Debit Card is the activation of the card and the set up and the use of the 3D Secure Password. The Provider has submitted a copy of the Complainant's Debit Card terms and conditions. Clause 2 of the terms and conditions of the Complainant's Debit Card provides, among other things, the following:

> *"2.0 Using your Card*
> *...*
> *2.2 These terms and conditions apply to your Card and tell you how it works.*
> *...*
> *2.6 When you receive your [named] Debit Card, you must activate it at one of our ATM's. If activation does not take place within 60 days of the issue of the Card, in the interest of card security, the card will be cancelled and a new card will have to be applied for. The activation of your Card is acceptance of these Card terms and conditions."*

The Provider submits that Clause 2(c) of the 3D Secure terms and conditions state:

> *"Use of a 3D Secure by creating a 3D Secure Password will represent your acceptance of these Conditions."*

The Provider submits that the Complainant set up her 3D Secure Password on 19 June 2015 while carrying out an online transaction, and in doing so agreed to the Terms and Conditions of use of 3D Secure. The Provider submits that the Complainant re-registered for 3D Secure on 21 September 2016 and set up a new password on this date.

Clause 14 of the terms and conditions of the Complainant's Debit Card provides, among other things, the following:

> *"14.0 Disputes or Unauthorised Transactions*
> *14.1 If there is a dispute about your Account or Card, you accept that the records kept by us or on our behalf are sufficient evidence of your Card's use. If a transaction is made using your Card with the PIN, the card reader in a Contactless transaction or the Verified by Visa service, you agree that we can conclude that the transaction was made by you*."

Regulation 70 of the 2009 Regulations places various obligations on customers. It provides the following:

> *"70. (1) The obligations of a payment service user entitled to use a payment instrument are-*
>
> *(a) of using the payment instrument in accordance with the terms governing its issue and use, and*
>
> *(b) of notifying the payment service provider that issued the instrument, or an entity specified by that payment service provider,* ***without undue delay***

/Cont'd…

on becoming aware of the loss, theft or misappropriation of the payment instrument or its unauthorised use.

(2) For the purposes of paragraph (1)(a), a payment service user shall, as soon as he or she receives a payment instrument, ***take all reasonable steps to*** *keep its personalised security features safe".*

The Provider submits that the Complainant failed to fulfil her obligations set out in Regulation 70 of the 2009 Regulations by giving her Debit Card details and confidential information to a third party to enable the third party set up a 3D Secure Password and the disputed transactions to be carried out.

I note that Clause 3 of the terms and conditions of the Complainant's Debit Card provides, among other things, the following:

*"**3.0 Protecting your Card, PIN and Verified by Visa Password***

...

3.2 You must keep the PIN and Verified by Visa Password secret, memorise them and take the greatest possible care to prevent anyone knowing them or using them fraudulently or without your permission, You should never write down the PIN or the Verified by Visa Password in a place where you also keep the Card or where it can be easily linked to your Card.

3.3 You will need your Verified by Visa Password to authenticate online (internet) debit card transactions with participating merchants.

3.4 You should always protect your Card and take the greatest possible care to ensure it is not lost, stolen or used in an unauthorised way.

3.5 If your Card is lost or stolen or you think someone knows your PIN, or your Verified by Visa Password, you must contact us immediately.

3.6 You are responsible for your Card and you must ensure that you protect it in line with this clause 3.0. If you do not do so, you will be liable for any loss suffered as a result."

I also note that on page 17 of the terms and conditions, under the heading "***6.0 Loss, Theft or other Misuse of your Card***", it states:

"6.1 You must tell us immediately if your Card is lost or stolen, if you suspect your Card has been used without your permission or if your PIN or Verified by Visa becomes known to someone else. You must inform us by contacting your branch or telephoning... We may ask you to confirm this notification in writing within seven days... You must not use the Card again.

6.2 You can limit your own losses if you tell us immediately when your Card has been lost, stolen or used without your permission. The same applies if you believe someone else knows your PIN or Verified by Visa Password.

6.3 If you use your Card as a Consumer, you are liable for only €75 in unauthorised transactions carried out on your Account before you reported the issue.

/Cont'd…

6.4 You are not liable for any transactions carried out after you report an issue with your Card.

6.5 You will be liable for the full amount of the unauthorised transactions if they were made:

(a) because of any fraud or gross negligence by you

(b) the Card was lost or stolen and the PIN/Verified by Visa Password became available to the finder or thief or someone else had access to the Card

(c) someone possesses the Card with your consent and uses it or gives it to someone else; or

(d) you do not co-operate fully with us or others in any investigation concerning the theft or loss of the Card or any attempt to retrieve it".

The "*3D Secure Terms of Use*" state underneath the heading "***CARDHOLDER RESPONSIBILITIES***", among other things, that:

"*(a) You alone are responsible for ensuring that your 3D Secure Password and other information is kept secure. You must keep the password secret, memorise it and take the greatest possible care to prevent anyone knowing it or using it fraudulently...*
(b) You must never allow another person to use your 3D Secure Password..."

Regulation 74 of the 2009 Regulations deals with "*Payment service provider's liability for unauthorised payment transactions*" as follows:-

"74.(1) In the case of an unauthorised payment transaction, the payer's payment service provider shall, if the payer concerned has given notice in accordance with Regulation 72 refund to the payer immediately the amount of the transaction and, if necessary, restore the debited payment account to the state it would have been in had the transaction not taken place.

..."

Regulation 74 must be read in light of the terms of Regulation 75 of the 2009 Regulations which provides as follows:

"Payer's liability for certain unauthorised payment transactions.
75. (1) Despite Regulation 74, and subject to paragraphs (2) to (5), a payer shall bear the loss relating to unauthorised payment transactions on the payer's account, up to €75 in total, if the transaction results from-

(a) the use of a lost or stolen payment instrument, or
(b) if the payer has failed to keep a payment instrument's personalised security features safe, its misappropriation.

(2) A payer shall bear all the losses relating to an unauthorised payment transaction if he or she incurred them by acting fraudulently or by failing,

/Cont'd…

intentionally or by acting with gross negligence, to fulfil one or more of his or her obligations under Regulation 70.

(3) A payer shall not bear any financial consequences resulting from the use of a lost, stolen or misappropriated payment instrument after giving notice in accordance with Regulation 70(1)(b), unless he or she has acted fraudulently.
..."

The Provider submits that by responding to the phishing email and divulging her Debit Card information details, albeit inadvertently, the Complainant failed to abide by the terms and conditions of her Framework contract, in particular Clause 6.5 of the Debit Card terms and conditions.

In the circumstance, given that the Complainant unfortunately, in error, responded to a phishing email, Provision 75(1) of the 2009 Regulations does not apply.

The Provider states that it "*is entirely satisfied that the conduct and activities of the Complainant constitute gross negligence on her part and further by acting in such a grossly negligent fashion by disclosing her personal security details to a third party, contrary to her obligations under the [named] debit card conditions of use. In essence the Complainant directly facilitated the transactions in question*". The Provider goes on to state that it "*further took account of the fact that there are many scams currently in existence whereby customers receive emails, phone calls and text messages purporting to be from legitimate companies or government bodies. Customers are asked to provide their personal security details thus enabling unknown third parties to carry out fraudulent transactions using the unsuspecting customer's personal security details. These scams are a well-known phenomenon that has been in existence for many years*". The Provider submits that it regularly advises customers of the dangers of such fraud.

The Provider submits that its website warns customers to be alert to unsolicited e-mails, phone calls and text messages and advises customers not to respond to these. The Provider submits that it will never send unsolicited e-mails or text messages to its customers asking for personal security information.

The Provider states, "*In light of the fact that such fraud attacks are now commonplace, when combined with the level of general media attention and both industry and Bank specific security warnings, the Bank is firmly of the view that by responding to the phishing email and providing her personal security details the Complainant clearly acted with gross negligence and facilitated the transactions in question*".

The Complainant submits that she was not aware that the Provider did not send out emails requesting information from its customers, and only became aware during the telephone conversation with the Provider's representative on 14 December 2016. The Complainant submits that her computer skills are very basic, and she does not look at the Provider's website, so would not be aware of phishing emails.

Regulation 73 of the 2009 Regulations provides the following:

/Cont'd…

> *"Evidence on authentication and execution of payment transactions*
> *73. (1) If a payment service user denies having authorised an executed payment transaction or claims that a payment transaction was not correctly executed, it is for the payment service provider concerned to prove that the transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other error or failure.*
>
> *(2) If a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider is not in itself necessarily sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or intentionally or failed, because he or she acted with gross negligence, to fulfil one or more of his obligations under Regulation 70"*

The Provider states that "*In this instance, the "payment instrument" in question is the Complainant's [named] debit card, and it is not the case that the Bank is solely relying on use of the [named] debit card, rather it is on the basis of the use of the [named] debit card ("payment instrument") in conjunction with the additional, and entirely separate, 3D Secure password that the Bank was satisfied that this transaction was authorised*". The Provider goes on to state "*Notwithstanding this, the Complainant subsequently advised the Bank that the transaction complained of was not carried out by her. However the Complainant also confirmed that she had supplied her [named] Debit Card details and confidential information to an unknown third party when she responded to the phishing email purporting to be from [online banking] and divulged her [named] Debit Card and confidential details which enabled a third party to undertake the disputed transactions*".

The Provider submits that its records are evidence that someone used the Debit Card details and a newly set up 3D Secure Password, set up using the Complainant's confidential information, to carry out the disputed transactions.

The Provider submits that it received the Complainant's complaint on 24 January 2017 by post, and the complaint was formally logged on its internal complaint handling system on that day. The Provider submits that its acknowledgment letter issued to the Complainant on 1 February 2017. In light of this delay, the Provider, in its submission to this Office dated 18 January 2018 offered the Complainant the sum of €250.00 in full and final settlement of the complaint.
Provision 10.9 (a) of the Consumer Protection Code 2012 provides that:

> *"a) the regulated entity must acknowledge each complaint on paper or on another durable medium within five business days of the complaint being received"*

Based on the evidence before me, I note that the Complainant's 3D Secure password was used to carry out the unauthorised transactions and the Complainant confirmed that she had responded to an email on 13 December 2016 purporting to be from the Provider. In my opinion, this disclosure of her security details constituted a breach of clause 3.2 of the

/Cont'd…

Complainant's visa debit terms and conditions, and, as a result, the Provider was entitled to refuse to refund the transactions pursuant to Clause 6.5.

Thereafter, I am obliged to consider whether the first Complainant's actions constituted "*gross negligence*" for the purposes of the 2009 Regulations. The term "*gross negligence*" is not defined in either the 2009 Regulations or its Parent Directive (Directive 2007/64/EC). Recital 33 of the Parent Directive states that:

> "*...in order to assess possible negligence by the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should be evaluated according to national law*".

I note that the concept of gross negligence was considered by both the High Court and the Supreme Court in the case of *ICDL Saudi Arabia v European Computer Driving Licence Foundation Ltd* [2011] IEHC 343; [2012] IESC 55. In this case the High Court set a test for gross negligence, that is "*...a degree of negligence where whatever duty of care may be involved has not been met by a significant margin*". This was approved by a majority of the Supreme Court.

Accordingly, I must examine the Complainant's actions to determine if she has acted with gross negligence by applying the significant margin test referred to above. I accept that the evidence before me indicates that the Complainant divulged her personal account information to an unauthorised third party, and that this action on her part inadvertently enabled the fraudster to remove the funds from her bank account by means of her debit card. By divulging her personal account information to an unauthorised third party, the Complainant did in my opinion, unfortunately act in a manner that constituted gross negligence, and I must accept that this gross negligence on the Complainant's part facilitated the carrying out of the unauthorised transactions on her account. I accept, therefore, the Provider was entitled to refuse to refund the transactions.

While I note that the Complainant submits that the unauthorised transactions were not debited from her current account until 16 December 2016, the transactions were carried out prior to the Provider becoming aware that these transactions had not been authorised by the Complainant. Once a transaction is correctly authorised, in this case by using the 3D Secure protocol, and the Provider is not on notice of any wrongdoing, the Provider must honour the transactions and cannot refuse to accept the charge when the merchants fully process the transactions. If this was not the case the entire card payment system could not operate, as it would mean that all transactions could be cancelled after they had been verified and approved.

Consequently, while I sympathise with the Complainant and I understand her frustration, it is my Legally Binding Decision that the complaint that the Provider wrongfully refused to reimburse the monies fraudulently withdrawn from her account, cannot be upheld. While I have sympathy for the Complainant's situation, the evidence shows no wrongful conduct on the part of the Provider in this regard, and rather, it is clear that the losses arose from the Complainant's error in responding to a phishing email. While I note that there was a slight delay on the part of the Provider in issuing a letter acknowledging the Complainant's

/Cont'd…

complaint, I am of the view that the Provider's offer of €250.00 is sufficient compensation in this regard. Given that the offer was made by the Provider prior to the adjudication of the complaint and on the basis that it remains available to the Complainant, it is my Legally Binding Decision that this aspect of the complaint will not be upheld.

Consequently, it is my Legally Binding Decision that this complaint is not upheld.

/Cont'd…

Conclusion

- My Decision pursuant to ***Section 60(1)*** of the ***Financial Services and Pensions Ombudsman Act 2017***, is that this complaint is rejected.

The above Decision is legally binding on the parties, subject only to an appeal to the High Court not later than 35 days after the date of notification of this Decision.

GER DEERING
FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

28 November 2018

Pursuant to *Section 62* of the *Financial Services and Pensions Ombudsman Act 2017*, the Financial Services and Pensions Ombudsman will publish legally binding decisions in relation to complaints concerning financial service providers in such a manner that—

(a) ensures that—

(i) a complainant shall not be identified by name, address or otherwise,

(ii) a provider shall not be identified by name or address,

and

(b) ensures compliance with the Data Protection Regulation and the Data Protection Act 2018.