An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

| | |
|---|---|
| **Decision Ref:** | 2020-0073 |
| **Sector:** | Banking |
| **Product / Service:** | Debit Card |
| **Conduct(s) complained of:** | Handling of fraudulent transactions<br>Dissatisfaction with customer service |
| **Outcome:** | Rejected |

## LEGALLY BINDING DECISION
## OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

The complaint concerns the Complainant's current account with the Provider and the fraudulent theft of funds therefrom.

### The Complainant's Case

The Complainant submits that she had recently completed a work placement scheme when, on 9 October 2018, she received a text message purporting to be from '*Revenue*' stating as follows:

> "*Dear Taxpayer, your refund is now available. Please click on http;//refund. Memberagency/refund. Refund amount €899.69 euro. Revenue Team".*

The Complainant subsequently followed the instructions in the text message to gain access to the alleged refund amount of €899.69. The Complainant submits that she then realised, on 12 October 2018, that her current account was missing €5,500 and that this amount had been transferred to [name of currency card redacted]. The Complainant submits that she telephoned Revenue and learned that the text message purporting to be from 'Revenue' was in fact fraudulent.

The Complainant submits that she contacted the local branch of the Provider whereupon she was instructed to contact its fraud department. The Complainant submits that, upon review, the Provider rejected her claim for the refund of her funds. The Complainant states that the Provider "*didn't red flag where my money was going, so it could have been prevented by getting confirmation from me when my money was withdrawn from my account that I was given my permission for this transaction"* [sic].

The Complainant further states that "I *know from speaking to people how* [other providers] *contacted them with suspicious activity and prevented these people from being the victim of fraud*".

The Complainant states that "*I am held responsible from been robbed by given out my details knowingly, which is totally untrue as I was not aware at the time that I was been robbed of my money*" [sic].

The complaint is that the Provider wrongfully refused to reimburse the monies fraudulently withdrawn from the Complainant's current account. The Complainant wants the Provider to return the €5,500 taken from her current account.

**The Provider's Case**

The Provider maintains that the transaction was completed using the Complainant's card and account details and her '3D Secure Password' or 'activation code', details which the Complainant provided having followed the link in the text message. The Provider maintains, by reference to the terms and conditions of the account, that it has no responsibility to indemnify the Complainant for the theft.

**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 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 4 February 2020, 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

/Cont'd…

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, within the period permitted, I set out below my final determination.

Prior to considering the substance of the complaint, it will be useful to set out certain terms and conditions of the current account as well as certain relevant legislation.

**Terms and Conditions of the Account**

The Provider relies on the following:

> ***6.0 Loss, Theft or other Misuse of 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 who had access to the Card.*

**Legislation**

The EU Payment Service Directive 2 ("PSD2") became law in Ireland in January 2018 with the signing by the Minister for Finance of the European Union (Payment Services) Regulations 2018 (Statutory Instrument No.6 of 2018). Regulation 96 of those regulations provides as follows (underlining added):

> ***Obligations of the payment service user in relation to payment instruments and personalised security credentials***
>
> *93. (1) A 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, and*
> >
> > *(b) notify the payment service provider concerned, or an entity specified by the latter for that purpose, without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument*

/Cont'd…

*(2) For the purposes of paragraph (1) (a), the payment service user concerned shall, in particular, as soon as it is in receipt of a payment instrument, take all reasonable steps to keep its personalised security credentials safe.*

Regulation 96 provides as follows (underlining added):

***Evidence on authentication and execution of payment transactions***

*96. (1) Where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, the burden shall be on the payment service provider concerned to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider.*

*(2) Where a payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge*

*(3) Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, including a payment initiation service provider as appropriate, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Regulation 93.*

*(4) A payment service provider, including, where appropriate, a payment initiation service provider, shall provide supporting evidence to prove fraud or gross negligence on the part of a payment service user.*

Regulation 97(1) provides as follows:

***Payment service provider's liability for unauthorised payment transactions***

*97.(1) Notwithstanding Regulation 95 and subject to paragraph (2), where a payment transaction is not authorised, the payer's payment service provider shall—*

> *(a) refund the payer the amount of the unauthorised payment transaction immediately, and in any event not later than the end of the business day immediately following the date that the payer's payment service provider notes or is notified of the transaction, except where the payer's payment service provider has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing*

/Cont'd…

*(b) where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place, and*

*(c) ensure that the credit value date for the payer's payment account shall be no later than the date the amount was debited*

Regulation 98(3) provides as follows (underlining added):

***Payer's liability for unauthorised payment transactions***

…

*(3) Notwithstanding Regulation 97, a payer shall bear all of the losses relating to an unauthorised payment transaction where the losses were incurred by the payer—*

*(a) acting fraudulently, or*

*(b) failing to comply with its obligations under Regulation 93 either intentionally or as a result of gross negligence on its part.*

**Analysis**

This is a most unfortunate case where the Complainant has found herself the victim of a phone scam resulting in the theft from her account of €5,500.00. I understand the Complainant's frustration and difficulty. She has acknowledged her own naivety but is of the view that the Provider should have done more to protect her from the exploits of the fraudsters.

In this case, the Complainant clicked on the link in the text message and was brought to a webpage where certain details were requested of her. The text message did not quote the real web address of Revenue.

Recordings of telephone calls between the Complainant and the Provider in relation to the matter have been provided in evidence. I have considered the content of these calls. It is clear from the recording of the phone call of 12 October 2018, the Complainant entered her personal account details in this webpage including her name, her account number and her card number. In addition, the Complainant inputted her '3D Secure Password' or 'activation code' which had been sent by text to the Complainant's mobile phone (this is a security measure to militate against fraud).

With regard to the text message sent to the Complainant providing her with the '3D Secure Password' or 'activation code', the Provider has stated that this message would have confirmed that the transaction involved was a "*purchase for Eur 5,500 at* [name of currency card redacted]." (The text message is sent from a secure system and a precise copy of it cannot be reproduced.) The Provider surmises that the Complainant did not read this text

/Cont'd…

properly. The Complainant has not taken issue with this assumption or denied the content of the text message.

It is abundantly clear that the Complainant thought that the text message purporting to be from 'Revenue' and the webpage linked to the text message were genuine and not fraudulent however this, unfortunately, was not the case and the details provided by the Complainant were in fact used to effect a fraudulent transfer of €5,500 out of the Complainant's account. The Provider cannot be held responsible for this unfortunate event.

The Complainant volunteered her personal details in the sense that she physically input them into the webpage albeit whilst operating under a false assumption that the text was genuinely a message from Revenue seeking to reimburse circa €900 to her. Thereafter, the Complainant provided her '3D Secure Password' or 'activation code' notwithstanding that the text message providing this code to the Complainant made clear that the intended transaction involved a purchase (rather than a refund) from an entity other than Revenue [name of currency card redacted], in the amount of €5,500 (that is an amount other than the figure the Revenue supposedly intended to refund).

The foregoing was unfortunately an act of what is described as 'gross negligence' on the part of the Complainant as described in the terms and conditions of the account and the relevant regulations and was an action for which the Provider cannot be held responsible. The conduct qualifies as 'gross negligence' as described in the PSD2 Regulations (reproduced above) and, by virtue of Regulation 98(3), the Complainant must bear all of the losses relating to the transaction. In this regard, I accept that the Complainant failed to keep her personalised security credentials safe. I also accept that the Provider has substantiated the instance of 'gross negligence' in accordance with Regulations 96(3) and (4).

The Complainant argues that the Provider did not 'red flag' where the money was going. However, I am not of the view that it was incumbent on the Provider to interrogate the destination for an online transaction in circumstances where several layers of security had already been satisfied. The Complainant complains that the Provider should have sought "*confirmation*" from her that she had 'given permission' for the transaction. However I accept that the provision by the Complainant of her account details together with the provision of the 3D password/activation code constituted, from the point of view of the Provider, an adequate communication of authorisation and permission from the Complainant.

I understand that the Complainant finds herself in a very difficult position of the unscrupulous people who defrauded her of her money. However, I cannot hold the Provider responsible.

Accordingly, for the reasons outlined above, I do not uphold this complaint.

/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 February 2020

**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.**