An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

Decision Ref:	2021-0382
Sector:	Banking
Product / Service:	Current Account
Conduct(s) complained of:	Handling of fraudulent transactions Dissatisfaction with customer service Failure to process instructions in a timely manner
Outcome:	Rejected

LEGALLY BINDING DECISION OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

This complaint arises out of a disputed transaction, which occurred on the **16th May 2020** on the Complainant's current account with the Provider.

The Complainant's Case

The Complainant states that on **16th May 2020** she received an email, from what appeared to be a courier/delivery company seeking payment of a €2.50 delivery fee. At the time she received this email, the Complainant had been expecting delivery of a package "*for over a month*". She submits that she received a communication to her phone requesting that she enter her One Time Passcode (OTP) to facilitate payment of the €2.50 courier payment.

The Complainant submits that "*within a few minutes*" of her entering the OTP for the payment, she discovered that a €919.85 transaction was displayed on her account as a payment to a third party and the amount had been debited from her account. She states that she immediately called the Provider to explain what had occurred and that the Provider informed her that it was a known scam which it was aware of.

The Complainant submits that she requested the Provider to block the transaction and that the Provider informed her that it would investigate the transaction and revert back to her. She notes that the disputed transaction was showing as pending on her account for 2 to 3 days thereafter.

The Complainant submits that the Provider subsequently contacted her informing her that she was liable for the transaction because she entered the One Time Passcode. It appears that this contact from the Provider was in the form of a letter dated **21 May 2020**. The Complainant submits that although she authorised the transaction under the "*false pretence"* that it was for a delivery charge of €2.50, she contacted the Provider "*within minutes".* She submits that the Provider was aware of the scam in question and that it made no effort to address the issue "*until after the transaction had completed*".

The Complainant asks why she does not have the right to "*block my money going to a fraudulent account".* She notes that the Provider's inability to do so may be understandable if "*several days"* had passed before it was notified of the fraudulent nature of the transaction, but the Complainant submits that it had "*ample time to address the issue and did not"*.

The Provider's Case

The Provider submits that upon receipt of the Complainant's complaint it referred the matter to its Fraud Investigations Team (FIT). The Provider states that its FIT advised that the transaction had been made prior to the Complainant reporting the debit card misuse to the Provider. It stated that the transaction was completed with the valid card details together with a valid One Time Passcode which would have been delivered to the Complainant by SMS text message.

The Provider states that its records show that during a call on **16 May 2020** the Complainant had stated that she had clicked the link and disclosed the One Time Passcode that issued to her phone. It submits that the text message containing the One Time Passcode contained the merchant name and the transaction amount, that the transaction could not have been completed without the third party fraudster also being in possession of this information. It submits that once the Complainant provided her details and the transaction was authorised, the Provider could not have prevented the transaction from processing. The Provider maintains, by reference to the terms and conditions of the visa debit card, that it has no responsibility to indemnify the Complainant for the theft.

The Complaint for Adjudication

The Complainant's complaint is that the Provider wrongfully failed to reimburse her in the amount of €919.85 in circumstances where the transaction undertaken on her account was fraudulent.

/Cont'd…

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 **6 October 2021**, 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, within the period permitted, the final determination of this office is set out below.

Chronology of Events

- **16th May 2020 at 1.03pm:** The disputed transaction is authorised by the Complainant entering a One Time Passcode
- **16th May 2020 at 1.50pm:** The Complainant phones the Provider reporting the disputed transaction and confirms with the Provider that it was a fraud. The Provider cancels the Complainant's card and informs the Complainant that she will be contacted by the Provider within 2 to 3 working days
- **21st May 2020:**
    - The Provider's agent telephones the Complainant in respect of its investigation into the disputed transaction. The Complainant admits to having authorised the transaction due to having not read the entirety of the SMS message issued to her by the Provider. The Provider's agent informs the Complainant that the Provider will contact her again to provide an update on the investigation.

/Cont'd…

  - The Provider's Fraud Investigation Team issues a letter to the Complainant informing her that she is liable for the disputed transaction.
- **3rd June 2020:** The Complainant lodges a complaint with the Provider.
- **17th June 2020:** The Provider issues its Final Response Letter.
- **27th June 2020:** The Complainant makes her complaint to this Office.

Evidence

(i) Visa Debit Card (Personal) Terms and Conditions

The following provisions are relied on by the Provider

3.0 Protecting your Card, PIN and other Security Credentials

"3.3 When making online transactions you may be required to enter a 3D Secure Passcode that will be sent to your mobile number we hold on file for you. To complete such a transaction you will need to enter the passcode provided. If you use the 3D Secure service, such use will constitute acceptance of the terms of use of 3D Secure. These terms of Use can be found at [Provider's web address].

If you use the 3D Secure service, you agree that we can conclude that the transaction was made by you. You must make sure that we have your up to date mobile phone number to send 3D Secure Passcodes because if we do not have a valid mobile phone number for you, you may not be able to use your Card for online transactions.

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 other Security Credentials, you must contact us immediately. You may advise us free of charge via the Freephone number listed on our website [Provider's web address]".

4.0 Using your Card for purchases and cash withdrawal

"4.1 When you carry out a cash withdrawal at an ATM or make a payment using your Card, we deduct the amount from your Account. You cannot stop a Card transaction.

/Cont'd…

4.2 You must make sure that a Card transaction including the amount is correct before you enter your PIN, 3D Secured Passcode or any other Secured Credential."

6.0 Loss, Theft or other Misuse of your Card

"6.3 If you use your Card as a Consumer, you are liable for only €50 in unauthorised transactions carried out on your Account before you reported the issue. If the loss, theft or misappropriation of the Card was not detectable to you then you will have no liability for any unauthorised transactions except where you have acted fraudulently.

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, 3D Secure Passcode or other Security Credentials 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.

6.6 In the event we suspect or detect any fraud or unauthorised activity on your Account, we may advise you and/or the relevant Cardholder via phone call, SMS message or email as appropriate. If we deem it necessary we may block or restrict your Account and/or any Card issued on the Account and may advise you and/or the relevant Cardholder of the block and how it may be removed."

9.0 Ending this Agreement and Interruption to Services

"9.2 We may end this agreement immediately or block any payments on your Account if:

/Cont'd…

(i) you die;
(ii) you are declared bankrupt or insolvent (under Irish or other law);
(iii) you seek legal protection from your creditors or enter a composition or settlement agreement with your creditors whether under a statutory scheme or otherwise;
(iv) you have failed security checks
(v) we have reason to suspect there is unauthorised or fraudulent activity on your Account even where we think you are innocent;
(vi) we are required to do so by law, regulation or direction from an authority we have a duty to obey;
(vii) you have breached these terms and conditions or the Account terms and conditions; or
(viii) your Account is overdrawn with an unauthorised overdraft or is operating in excess of your agreed overdraft permission".

(ii) Personal Current Account Terms and Conditions

12.0 Incorrect, Disputed or Unauthorised Transactions

"12.2 You must tell us about any transaction that was not (a) authorised by you or on your behalf (for example, was not authorised by you through a TPP), or (b) done correctly, as soon as possible but no later than thirteen months after the date of the transaction, You can notify us for free of using the Freephone number listed on our website [Provider's web address]".

12.4 If payment is made from your Account that was not authorised by your or on your behalf, (for example through a TPP), we will, subject to 12.5 and 12.6, refund your Account and restore it to the way it would have been if the unauthorised payment had not happened. If it is later determined that no refund should have been paid we will be entitled to recover it from your account without reference to you.

12.5 If any unauthorised payments came about because a payment instrument (for example, your card, number or code) was lost, stolen or misappropriated, and this is reported to us as soon as possible after you become aware of it, the maximum you will have to pay is €50. If the loss, theft or misappropriation of the payment instrument was not detectable to you then you will have no liability for any unauthorised transactions except where you have acted fraudulently.

/Cont'd…

12.6 You will be liable for the full amount of the unauthorised payments if they were made because of any fraud by you, or because you failed intentionally, or by behaving with gross negligence, to fulfil your obligations under these terms and conditions.

12.7 If any authorised transactions on your Account are incorrectly executed because of any acts or omissions by us, we will refund the transaction and restore your Account to the way it would have been if the transaction had not happened."

12.10 If we suspect or detect any fraud or unauthorised activity on your Account, we will advise you by phone call, SMS message or email as appropriate unless doing so would break the law. If we deem it necessary we may block your Account and will advise you of the block and how it may be removed".

23.0 Ending this Agreement and Interruption to Services

"23.4 We may close your Account immediately or block any payments from it if:

(i) you die or lose contractual capacity;
(ii) you are declared bankrupt or insolvent (under Irish or other law);
(iii) you seek legal protection from your creditors or enter a composition or settlement agreement with your creditors whether under a statutory scheme or otherwise;
(iv) you have failed security checks
(v) we have reason to suspect there is unauthorised or fraudulent activity on your Account even where we think you are innocent;
(vi) we are required to do so by law, regulation or direction from an authority we have a duty to obey;
(vii) the balance on your Account is between zero and €10.00 and you have not carried out an account transaction on it for a period of 12 months or more; or
(viii) you have breached these terms and conditions"

(iii) 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***

/Cont'd…

2018 (Statutory Instrument No. 6 of 2018). I have set out the parts of this legislation most relevant to the current complaint below:

Regulation 76(e) sets out the obligations of '*payment service providers'*, such as the Provider in the present case, to provide "*payment service users'*, such as the Complainant, with information on "*safeguards and corrective measures*" in respect of "*payment instruments*". The relevant payment instrument in this case was the Complainant's visa debit card. The Regulation states as follows:

> "*76. A payment service provider shall provide the following information to a payment service user:*
>
> *(i) where applicable, a description of the steps that the payment service user is to take in order to keep a payment instrument safe and how to notify the payment service provider for the purposes of Regulation 93(1)(b);*
>
> *(ii) the secure procedure for notification of the payment service user by the payment service provider in the event of suspected or actual fraud or security threats;*
>
> *(iii) if agreed, the conditions under which the payment service provider reserves the right to block a payment instrument in accordance with Regulation 92;*
>
> *(iv) the liability of the payer in accordance with Regulation 98 including information on the relevant amount;*
>
> *(v) how and within what period of time the payment service user is to notify the payment service provider of any unauthorised or incorrectly initiated or executed payment transaction in accordance with Regulation 95 as well as the payment service provider's liability for unauthorised payment transactions in accordance with Regulation 97;*
>
> *(vi) the liability of the payment service provider for the initiation or execution of payment transactions in accordance with Regulation 112;*
>
> *(vii) the conditions for refund in accordance with Regulation 100 and 101;*

Regulation 93 sets out the relevant obligations of the '*payment service* user(s)' in relation to payment instruments such as the Complainant's debit card.

/Cont'd…

Regulation 93 states in that regard:

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 less, theft misappropriation or unauthorised use of the payment instrument"

(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 states as follows:

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

/Cont'd…

(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 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

(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 provides as follows:

Payer's liability for unauthorised payment transactions

"98. […]

/Cont'd…

(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.

(iv) Audio Evidence

Audio evidence of telephone calls that took place between the Complainant and Provider was submitted to this office as part of this complaint. I have listened to the audio evidence and I note the following exchanges.

On **16th May 2019,** the date the disputed transaction took place, the following exchange took place:

Provider's Agent: *What we'll do is, we'll do an investigation, so we will look into these transactions for you and we will be back in contact with you in a couple of days*

Complainant: *I mean, that was [Courier company], now obviously it wasn't and I didn't look…I was looking for the passcode from [Provider] so I didn't look at the rest of the message, and then I looked again and it was like nine hundred and something euro, like…*

On **21st May 2019,** the Provider's agent telephoned the Complainant to ascertain information surrounding the disputed transaction:

Provider's Agent: *In or around that date*, did you receive any contact – a text message, an email or a phone call from anybody asking you to provide them with card information?

Complainant: *There was an email, which stated from what I thought was [Courier company], stated that there was insufficient information about my address and the package that I'm waiting for is in Dublin at that moment and I would have to pay €2.50 to bring to my home. So in order of that, I didn't think much about it, I just thought maybe there was something there…you know, it was €2.50, I didn't question it, and*

/Cont'd…

> *once everything was over, I looked back at the* [Provider] *message – the verification number, which I gave them, but I hadn't read the rest of the message. And when I read it after, a few minutes later, it said that €919.85 was taken instead of…€2.50*

*(v) Final Response Letter dated **17th June 2020***

In its Final Response Letter, the Provider upheld its decision to hold the Complainant liable. The Provider stated the following:

> "*The One Time Pass Code is issued by text message to your mobile phone for additional security. This text message contained the merchant name and the transaction amount. The transaction could not be completed without the fraudster also being in possession of this information.*
>
> *Please be advised that once you provided your details and the transaction was authorised, the Bank could not have stopped the transaction from processing to your account. I respectfully refer you to the terms and conditions of your Visa Debit Card […]*
>
> *Please note that once a successful authorisation is processed, the Bank does not have the authority to stop or block any transaction. A transaction authorisation is requested by the merchant which then activates a request for a One Time Passcode (OTP) to be issued by* [Provider]*. Once this OTP is used, the transaction is approved. This action alone provides the* [Provider] *with information that the transaction was securely authorised by you as per the terms and conditions above."*

Analysis

This is an unfortunate case where the Complainant has been the victim of a scam resulting in the loss from her current account of **€919.85**. This was, no doubt, upsetting and difficult for the Complainant. She has admitted that she authorised the transaction in question but she submits that the Provider could have done more to address the issue, to inform her as to where her money had gone, and to protect her money from the fraudsters.

In this instance, I note that the Complainant entered the One Time Passcode she received from the Provider and supplied it through the fraudulent email communication which purported to be from a courier company. As part of this complaint, audio evidence of the two telephone calls between the Provider and Complainant in respect of this issue, has been made available.

/Cont'd…

It is apparent from the content of both of these calls that the Complainant acknowledges that she authorised the payment, by inputting the One Time Passcode or '3D Secure Password' which had been sent by SMS text message by the Provider, to the Complainant's phone. The Provider has outlined in its submissions that the provision of these passcodes is an added security measure in place to protect its customers from fraud.

It is apparent from the evidence submitted that the SMS text message sent to the Complainant's phone stated that the transaction it was requesting the Complainant to confirm, was for the amount of **€919.85**. It is obvious, from listening to the audio evidence in particular, that the Complainant truly thought that the email in question was from a legitimate courier company. However, this was not the case and the OTP, once supplied by the Complainant to the merchant, facilitated an authorised transfer of €919.85 from her account. The Provider cannot however be held responsible for this unfortunate and upsetting event, because the Provider did nothing wrong, and in fact before releasing the monies from the Complainant's account, it sought specific confirmation from her that the transaction was authorised, by requiring her to use the One Time Password, to facilitate payment.

The Complainant voluntarily entered the One Time Passcode or 3D Secure Password (in addition to her home address, as she confirmed during the telephone call of **21st May 2019**) into the webpage, notwithstanding that the message she received from the Provider stated that the transaction was for €919.95, a much more significant amount than she was intending to pay.

I am of the view that that the Provider was entitled in those circumstances, to take the view that the payment was authorised, whether intentionally by the Complainant or as a result of her 'gross negligence' as anticipated by the PSD2 Regulations, or as described in her Current Account Terms and Conditions and Debit Card Terms and Conditions, details of which are also set out above.

The Complainant states that

> "[the Provider] *made no effort to address the issue until after the transaction had completed, my issue is that even though I gave permission under false pretences to transfer the money, why do I not have the right to block my money going to a fraudulent account. I feel the bank could have done more to protect my money."*

I am not satisfied that the Provider was required to further question the payee account, when multiple layers of security had been satisfied.

/Cont'd…

The Provider has clearly set out both in its submissions in respect of this complaint, and in the relevant terms and conditions set out above, that a card transaction cannot be stopped once the One Time Password is entered. The evidence confirms that it is the responsibility of the Complainant to ensure that a card transaction, including the amount, is correct before entering a 3D Secured Passcode or any other security credential. I am satisfied that the Complainant's entry of the One Time Passcode into the webpage could reasonably be regarded by the Provider as sufficient communication of her authorisation and consent.

I understand that the Complainant is in a difficult and frustrating situation due to the fraudsters' actions. However, in the absence of any wrongdoing on the part of the Provider, I am satisfied that there is no reasonable basis upon which this complaint can be upheld.

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.

MARYROSE MCGOVERN
Deputy Financial Services and Pensions Ombudsman

29 October 2021

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.