



<u>Decision Ref:</u>	2022-0290
<u>Sector:</u>	Banking
<u>Product / Service:</u>	Money Transfer
<u>Conduct(s) complained of:</u>	Handling of fraudulent transactions Complaint handling (Consumer Protection Code)
<u>Outcome:</u>	Rejected

LEGALLY BINDING DECISION OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

The complaint concerns a disputed transaction where a third party debited a total of €1024.67 (one thousand and twenty-four euro and sixty seven cent) from the Complainant's account.

The Complainant's Case

The Complainant received an email on **24 April 2020** at 18:07 from an address purporting to be a courier service that advised her that action was required, in order to have a parcel re-delivered. Upon clicking on the link included, the Complainant says that she was informed that an additional charge of €2.50 (two Euro, fifty cent) was required in order to commence the re-delivery. She states that this email communication happened to coincide with her waiting for the return of an item from the repair section of an electronics company.

The Complainant sought to pay the fee with her debit card, held on her account with the Provider, but that she was unsuccessful in obtaining a One Time Password (OTP). The Complainant explains that she then used her credit card held with the Provider, and received a OTP for the transaction. The Complainant states that as she *“took it to relate to the perceived redelivery fee”* and she *“failed to notice that the amount and payee were different”*.

The Complainant states that, on **28 April 2020** at 09:23, she checked her bank balance with the Provider and found a transaction on her credit card that she did not recognise, amounting to **€1,024.67**. The Complainant states that she immediately contacted the Provider and cancelled the card, and the matter was referred to the Provider's fraud

department where she understood the transaction in question would be cancelled or frozen, pending the outcome of the investigation.

The Complainant states that on **29 April 2020**, she received a telephone call from the Provider's fraud department during which the details of the transaction were discussed and the avenues through which a third party could have accessed her payment card.

She states that during this call, she pointed out that she had been declined authorisation and that she had not been furnished with an OTP from the Provider in respect of her debit card, but had received an OTP for her credit card, which led her to believe that the transaction was valid. She states that it was on the reassurance of receiving a security code from the Provider, via text, that she selected and clicked on pay.

The Complainant states she:

“stressed how careful I had been and suggested if there had been a tighter security firewall for checking legitimate requests then I would not have clicked on PAY and thereby authorised the transaction.”

She states that there was no intention by her to authorise that specific transaction.

The Complainant states that she received the results of the Provider's investigation by post on **5 May 2020** *“effectively finding me responsible for the transaction”*. The Complainant states that the Provider did not furnish her with an email address to send further documentation. She did not have access to a printer, and states that it was very inconvenient and daunting to secure access to a printer, in the circumstances of social distancing and travel restrictions caused by the COVID-19 pandemic

The Complainant contends that the Provider did not sufficiently investigate or take appropriate action after she had notified it to cancel the transaction, and that the Provider should implement a better and more intuitive system where the Provider would work in tandem with the retailer, to flag that the purchased goods were to be delivered to a different address that did not fit the Complainant's profile of previous purchases. The Complainant states that the Provider's OTP is *“clearly inadequate as a security device”*, and that as a result, she feels that she was treated very badly by the Provider. She says that the Provider:

“have not shown a proper duty of care to me as a customer to protect my interests and to recover the funds that were effectively stolen from my credit card.”

The Complainant further asserts that, despite her contacting the Provider within hours of the breach of the security system, its inaction towards her was evident and that the Provider's failure to take responsibility was *“remarkable”*.

The Complainant wants the Provider to reimburse the sum of €1,024.67, minus the €2.50 validated by an OTP, to be credited to the payment card the Complainant holds with the Provider.

/Cont'd...

The Provider's Case

The Provider sent a letter on **29 April 2020** stating that it noted that the OTP transaction was made, prior to the report of the misuse of the card, and was completed using a combination of the Complainant's card details together with the valid OTP which was delivered to her by text message.

Based on this, the Provider states that since it is not possible to make such a transaction (without being in the possession of both the card details and the relevant verification method such as the OTP) it found that the Complainant was liable for the transaction.

This letter further stated that it reviewed the telephone conversations between the Provider's card security agents and the Complainant on **28 April 2020** and **29 April 2020** and noted that she had stated that she received a text message purporting to be from a courier service, and she clicked on the link and entered her card details and the OTP. The Provider further contends that the Complainant stated during her telephone conversations that she failed to take reasonable precautions to keep the information in relation to her card safe, as required under the Conditions of Use of the card.

On **20 May 2020**, the Provider issued a Final Response Letter. This letter again stated that it noted that the Complainant confirmed she had received a text from a third-party purporting to be the relevant courier. This letter also states that the Provider noted that the Complainant responded to the text message, and clicked on the link provided and entered her account details as she believed the message to be genuine. The Provider states that its Fraud Investigation Team has also advised that the above transaction was made, before the misuse of the card was reported to the Provider.

The Final Response Letter states that the OTP is issued by text message to the Complainant's mobile phone, for additional security. The text message contains the merchant name and the transaction amount and the transaction could not be completed without the fraudster also being in possession of this information.

The Provider says that once the Complainant provided her details and the transaction was authorised, it could not have stopped the transaction from processing to her account. The Final Response Letter relied on clause 3, 6 and 14 of the of the Complainant's debit card terms and conditions, in support of this.

The Provider states that when it is notified of a potential fraudulent transaction on a customer's credit card, its obligation is first to prevent any further fraudulent transactions where possible, and then to determine whether to refund the relevant transaction, having regard to the terms and conditions applicable to the use of the card. The Provider has also stated that should the Complainant consent to the Provider's cooperation with An Garda Síochána, the Provider will "*of course*" provide whatever assistance and information is required. However, the Provider states that is not obliged to conduct a "*quasi-criminal investigation*".

/Cont'd...

The Provider states that the transaction was authorised using the Complainant's credit card details and the OTP which she disclosed to the fraudster. The Provider states that the Complainant admitted herself that she did not read the OTP text message sent to her mobile telephone. The Provider states that these text messages are part of the Provider's fraud prevention procedures, and *"if customers decline to read them before authenticating transactions, they bear the responsibility for any losses that might arise"*.

In a further letter dated **18 February 2021**, the Provider reiterated its position that the Complainant was liable for the fraudulent transaction. However, this letter states that having reviewed the file afresh, the Provider acknowledges that its Final Response Letter of 20 May 2020, incorrectly quoted the terms and conditions for a visa debit card, and not the credit card account. The Provider states that at the time of the disputed transaction, the terms and conditions applicable to the use of the Complainant's credit card were those set out in the Classic and Platinum Credit card agreement which was effective from **April 2019** (the "Credit Card Terms and Conditions").

The Provider cited the correct Credit Card Terms and Conditions in this letter of 18 February 2021, and *"as a gesture of goodwill"*, and by way of apology for any confusion caused as a result of the misinformation, the Provider offered the Complainant **€250** (two hundred and fifty euro) in full and final settlement of the complaint.

The Complaint for Adjudication

The complaint is that, in **April 2020**, the Provider, without Complainant's authority, wrongfully allowed a third party to debit a total of €1,024.67 to her credit card account and since then has wrongfully failed to refund the Complainant's account.

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.

/Cont'd...

A Preliminary Decision was issued to the parties on **5 August 2022**, 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.

The chronology of events is noted as follows:

Friday 24 April 2020	The Complainant used her credit card details and the OTP sent to her mobile phone number, to progress a transaction on her account. The Complainant believed she was paying €2.50 for the re-delivery of a parcel by a Courier company.
Tuesday 28 April 2020	After checking her balance on her credit card, the Complainant noticed the transaction which she did not recognise. She telephoned the Provider and cancelled her card.
Wednesday 29 April 2020	The Complainant received a telephone call from the Provider's fraud investigation team (detailed below).
Wednesday 29 April 2020	A letter was issued from the Provider to the Complainant indicating that she was liable for the disputed transaction because she had authorised the payment through the OTP.
Friday 15 May 2020	The Complainant issued a letter to the Provider.
Wednesday 20 May 2020	A Final Response Letter was issued by the Provider to the Complainant.
July 2020	The Complainant made a complaint to this Office
Thursday 18 February 2021	The Provider issued a further letter to the Complainant outlining that it had incorrectly cited the terms and conditions for the debit card, rather than the credit card, in its earlier Final Response Letter.

I note that on **28 April 2020**, the Complainant telephoned the Provider and reported the transaction on the credit card. The Complainant stated that she did not receive any suspicious emails or text messages looking for her details.

/Cont'd...

On **29 April 2020**, an agent from the Provider's fraud investigation team telephoned the Complainant to follow up on the transaction on her credit card. The agent stated that the Provider had sent an OTP to the Complainant's mobile telephone "*to be entered on the website to verify the payment*", and asked if the Complainant had received this text, to which she initially stated "*no*", before clarifying that the "*code came in for my [credit] card*" for "€2.50" for the redelivery of an item that she had purchased.

The Complainant further stated that she was provided with a link on the text message, and the website link then asked for her credit card details and again stated that it was "*waiting on a code to come through*", which "*did come in for my [credit] card*". The Provider's agent explained that the text message sent to her phone was a "*scam*" and the fraudsters "*took the card details*". She also stated as follows:

"I'm in such a rush to use the code, usually you only see it coming in a banner on top... you don't actually read the thing... I never, ever saw that [third party seller], you know... but, again, as you said... I usually see it in the banner on top of the thing, and you just enter the code, and you don't think about it again."

I also note that in a letter dated **15 May 2020** to the Provider, the Complainant stated that:

"I had received a OPB from the [Provider] for the use of my [credit card] whereby I was led to believe that that the transaction was valid. It was on the reassurance of receiving security code from [the Provider] via text that I selected and clicked on pay".

- Relevant 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) (hereafter referred to as "the Regulations").

I have set out the parts of these Regulations 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 instance, 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 credit card.

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 loss, 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

/Cont'd...

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 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*

/Cont'd...

(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. [...]

(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."

In respect of the issue of "gross negligence", the Provider relies on the significant margin test identified in *ICDL Saudi Arabia v. European Computer Driving Licence Foundation Ltd* [2012] IESC 55, [2012] 3 IR 327 where at paragraph 59 of the Supreme Court Judgment, the Court cited Clarke J., noting that he concluded that the term 'gross negligence' meant a "degree of negligence" involving a "breach of the relevant duty of care by a significant margin." I accept that this explanation of gross negligence, is relevant to the wording in the Regulations.

- Relevant terms and conditions

Clause 15 of the Provider's Credit Card Terms and Conditions states:

"... The 3D Secure passcode or some other security credential may be required by us or a retailer to authorise credit card transactions..."

Clause 13 (h) states:

"If you use the 3D Secure service, you agreed that we can conclude that the transaction was made by you."

The definition section of the Credit Card Terms and Conditions also outlines the following regarding security credentials:

"Security Credentials' means the personalised security features we require you or an Additional Cardholder to use now or in the future to (a) access your Account through our online, phone and mobile banking channels; and (b) to authorise an account transaction. Sometimes we will give you the Security Credentials; in other cases we will ask you to choose them.

/Cont'd...

These are examples of Security Credentials; a personal identification number (PIN), password, one time pass code (such as a 3D Secure Passcode), security number or code (for example, those generated by a physical or digital security key), a response to a push notification, your registered device, your fingerprint or other distinctive personal characteristics, or any combination of these features or other ones we require now or in the future...

'3D Secure' means a system used as an added layer of security for credit card transactions. Examples include, Verified by Visa and Mastercard Securecode™...*

'3D Secure Passcode' means your one time passcode sent to your mobile phone by text message (SMS) for use on 3D secure which you may need to complete a purchase using your Credit Card."

Clause 6(ii) sets out the Complainant's responsibility with regards to security credentials:

"You must... always protect the Credit Card. Take all reasonable precaution to ensure the Credit Card and any Security Credential is not lost, mislaid or stolen..."

Clause 13 states:

- (c) In the event of an authorised transaction out of the account, the bank will, subject to 13(d) and 13(e) below, refund the amount of such unauthorised transaction and will restore the account to the state it would have been in but for the unauthorised transaction.*
- (d) where such unauthorised transactions have resulted from the loss, theft or misappropriation of the Credit Card, PIN or 3D Secure Passcode or any other Security Credential where it was reported to the Bank without undue delay you will be liable for such unauthorised transactions up to a maximum of €50, except where it was undetectable to you, in which circumstances you will have no liability.*
- (e) where any unauthorised transactions arise as a result of any fraud by you, or because you have failed intentionally, or because of gross negligence on your part to fulfill your obligations under these Conditions of Use, you shall be liable for the amount of such unauthorised transactions."*

Analysis

I note that on **24 April 2020**, the Complainant was sent an email from a fraudster (often known as a “phishing” scam). It appears this fraudster pretended to be a third-party courier service and asked the Complainant to insert her card details. The Complainant believed this was to facilitate payment of €2.50 for re-delivery of an item she had purchased, however, it was to authorise payment of the sum of €1,024.67.

The Provider has stated that this required authentication using a One Time Password (OTP). I note that the following text was sent by the Provider to the Complainant's mobile number:

*“510*** is your [credit card] SecureCode one-time passcode. Use it within 5 minutes to Complete your purchase for GBP873.16 at [third party seller].”*

I note that during the telephone call dated **29 April 2020**, and in a later letter dated **15 May 2020**, the Complainant stated that she entered the OTP, thinking it was for the redelivery fee of €2.50.

The Provider states:

“It is respectfully submitted that the Provider was entitled to view the disputed transaction as properly authorised by the Complainant, in which case she was properly held liable for same and not entitled to a refund. Alternatively, the Provider was entitled to take the view that the disputed transaction, though unauthorised in one sense, arose due to the Complainant's failure to keep her card details and OTP safe, thereby breaching the Credit Card Terms and Conditions. It is respectfully submitted that the Complainant's disclosure of these details to the fraudster represents a failure to meet the duty of care she owed, by a significant margin. In these circumstances, she was guilty of gross negligence and was accordingly held liable for the disputed transaction.”

On the basis of the evidence available, I am of the view that the Provider was entitled to form the opinion that the payment was authorised by the Complainant, given her use of the OTP to authorise the specific transaction in question, on **Friday 24 April 2020**.

The Provider has clearly set out both in its submissions in respect of this complaint, and in the Credit Card Terms and Conditions set out above, that a card transaction cannot be stopped once the OTP 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 her 3D Secure Passcode or any other security credential.

I am satisfied that the Complainant's entry of the OTP into the webpage could reasonably be regarded by the Provider, as sufficient communication of her authorisation and consent. In those circumstances, I do not accept, as suggested by the Complainant, that the Provider wrongfully permitted the debit of funds by the third party to her account on 24 April 2020.

/Cont'd...

Neither do I accept that the Provider acted unreasonably in failing to refund the amount of the transaction to her account, given that the transaction had been authorised by the Complainant on the day in question.

I note, the Provider has also accepted that the Final Response Letter dated **20 May 2020**, erroneously made reference to terms and conditions which did not apply to the Complainant's credit card at the relevant time. The Provider stated:

"When this error was rectified by the Provider in its letter dated 18 February 2021, it is acknowledged that the error represents a lapse in customer service such that a monetary gesture is warranted. It is in these circumstances that the sum of €250 was offered to the Complainant as a goodwill gesture in full and final settlement of the present complaint. Please note that this offer remains open to the Complainant should she wish to accept it."

The relevant section of the Consumer Protection Code 2012 (the CPC 2012) states at section 2.8 that the Provider must ensure that it *"corrects errors and handles complaints speedily, efficiently and fairly"*. Section 2.2 also states the Provider must act *"with due skill, care and diligence in the best interests of its customers"*.

I am satisfied that this reference to the debit card terms and conditions, would have confused matters as the issue concerned her credit card. Therefore, I take the view that the Provider was in breach of section 2.8 and 2.2 of the CPC 2012, but I note that in responding to the investigation by this Office, the Provider recognised that error and I am satisfied that the monetary compensation offered, of **€250** is satisfactory in the circumstances. Accordingly, it will be a matter for the Complainant to make direct contact with the Provider, if she wishes to accept the compensatory gesture and I do not consider it appropriate or necessary to make any direction to the Provider in that regard.

I understand that the Complainant is in a difficult and frustrating situation, due to the fraudster's actions. She was unfortunately the victim of a phishing email from the fraudster, and I have every sympathy for her, for the position which she had found herself, having been tricked into believing that she was authorising a much smaller amount.

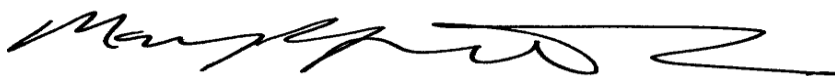
The Provider's One Time Password text was, however, very clear in its contents and I am not satisfied that the Provider did anything wrong such that it should bear the responsibility for the cost incurred by the Complainant's actions in authorising the payment in question. In the absence of any wrongdoing on the part of the Provider, I am satisfied that there is no reasonable basis upon which the 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.

/Cont'd...

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
FINANCIAL SERVICES AND PENSIONS OMBUDSMAN (ACTING)

29 August 2022

PUBLICATION

Complaints about the conduct of financial service providers

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.

Complaints about the conduct of pension providers

Pursuant to *Section 62* of the *Financial Services and Pensions Ombudsman Act 2017*, the Financial Services and Pensions Ombudsman will **publish case studies** in relation to complaints concerning pension 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.