



<u>Decision Ref:</u>	2021-0215
<u>Sector:</u>	Banking
<u>Product / Service:</u>	Current Account
<u>Conduct(s) complained of:</u>	Disputed transactions
<u>Outcome:</u>	Upheld

LEGALLY BINDING DECISION OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

This complaint relates to an unauthorised transaction on the Complainant's account and the Provider's refusal to indemnify the Complainant for the losses incurred arising out of the unauthorised transaction.

The Complainant's Case

The Complainant is a limited company. The Complainant's principal (for ease of reference also referred to below as the Complainant) was abroad in [European Country] and states that on **20 September 2019**, he used his debit card associated with the account held with the Provider whilst in a bar. He states that this led to 1 unauthorised transaction on his account totalling €500.

The Complainant submits that on the date in question, he had a number of cards on his person/in his card pouch which were connected to a number of different accounts. The Complainant states that he used his debit card connected to his account ending 850 in a handheld card machine at the bar. He states that he practiced due care with his card when making the payment at the bar and thereafter put his card into his pouch.

The Complainant submits that the following day, he checked his account online and became aware of the unauthorised transaction and the money that had been debited from the Complainant's account.

The Complainant states that he had not received any notification from the Provider nor any indicator that the transaction had been flagged by the Provider. The Complainant still had possession of the card. The Complainant notified the Provider on **21 September 2019** and the Provider cancelled the card and stated that the matter would be investigated by its card fraud investigation team. The Provider advised the Complainant to report the matter to the local police station.

The Provider declined to refund the money taken from the Complainant's account on the basis that the transaction had been carried out using the Visa debit card in conjunction with the associated PIN and as per the terms and conditions of the contract with the Provider, such transaction was considered to be correctly authorised.

The Provider's Case

The Provider states that the terms and conditions of the contract in place with the Complainant stipulate that the transaction is considered to be correctly authorised and therefore the Complainant is liable for the transaction.

In addition, the Provider has stated that it will not refund the losses incurred because it disputes that the transaction was unauthorised.

The Provider also says that even if it was unauthorised, then given the security measures put in place by the Provider, the Complainant must have allowed a third-party access to this security information and in doing so, he failed to comply with his framework agreement and breached the European Communities (Payment Services) Regulations 2018.

The Provider asserts the Complainant's actions amounted to gross negligence within the meaning of the European Communities (Payment Services) Regulations 2018.

The Complaint for Adjudication

The complaint is that the Provider wrongfully, unreasonably and through a mistake of law or fact refused to indemnify the Complainant for the unauthorised debit to the account. The Complainant is seeking a refund of all the monies taken from the account as a result of the fraud.

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 Company 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.

/Cont'd...

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 **28 May 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 substantive submissions from the parties, within the period permitted, the final determination of this office is set out below.

At the outset, the Provider has acknowledged in its submission to this office that the transaction carried out was subject to the provisions of the European Communities (Payment Services) Regulations 2018 (the “2018 Regulations”) and this Office is satisfied that the 2018 Regulations are relevant to this complaint. The 2018 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 (ie. physical devices (such as cards) and/or [a] set of procedures).

In this matter, the Complainant denies that it authorised the disputed transaction. The Provider disputes that the transaction was unauthorised and says that if it was, then the only other explanation is that the Complainant enabled its visa debit card including the visa debit PIN to be shared with another party who was not authorised to have such information.

Regulation 96 (3) of the 2018 Regulations provides:

(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.

[my emphasis]

In light of the foregoing provision and in the circumstances of this matter, this Office does not accept that the mere use of the card is evidence that the transaction was authorised.

/Cont'd...

On the night of 20 September 2019 or the morning of 21 September 2019, a transaction was processed from the Complainant's account which the Complainant states was not authorised. It is relevant to note that the transaction was carried out by use of a visa debit card and associated PIN.

The Provider explains that the transaction was carried out in a bar and was completed using chip and PIN with the card being present and I accept that this is evidenced by the association with the point-of-sale code POS 05: "CHIP AND PIN PRESENT AND VERIFIED", apparent from the documentary evidence.

Regulation 93 (1) of the 2018 Regulations places a number of obligations on customers in relation to payment instruments and personalised security credentials:

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.

It is also necessary for the Complainant to use the debit card in compliance with the terms and conditions agreed with the Provider.

3.0 Protecting the Card, PIN and other Security Credentials

3.1 The Cardholder must sign the Card immediately on receipt.

3.2 The Cardholder must keep the PIN secret, memorise it and take the greatest possible care to prevent anyone knowing it or using it fraudulently or without the Cardholder's permission. The Cardholder should never write down the PIN in a place where the Card is kept or where it can be easily linked to the Card.

3.3 When making online Cardholder Transactions you may be prompted to enter a 3D Secure Passcode that will be sent to the mobile number we hold on file for you. To complete such a Cardholder 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 and of 3D Secure. These terms of Use can be found at [Redacted] 3DSecureTermsOfUse. 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 The Cardholder must always protect the Card and take the greatest possible care to ensure it is not lost, stolen or used in an unauthorised way.

3.5 If the Card is lost or stolen or the Cardholder thinks someone knows the PIN, or other Security Credentials the Cardholder must contact us immediately. We can be contacted free of charge via the Freephone number listed on our website [Redacted]

3.6 The Cardholder is responsible for the Card and Security Credentials and must ensure that they are protected in line with this clause 3.0. If the Cardholder does not do so, the Cardholder may be liable for any loss suffered as a result.

3.7 The Cardholder must ensure that the Bank is immediately informed of any change in the Cardholder's place of business. If this is not done it may not be possible for the Bank to investigate disputed or fraudulent transactions on the Account.

...

6.0 Loss, Theft or other Misuse of your Card

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, 3D Secure Passcode or other Security Credentials becomes known or is in possession of someone else. You must inform us by contacting your branch calling us free of charge via the Freephone number listed on our website [Redacted]. We may ask you to confirm this notification in writing within seven days (or 21 days if you are abroad). You must not use the Card again.

6.2 You must tell us about any transaction that you did not authorise, or any transaction that was not done correctly, as soon as possible but no later than thirteen months after the date of the transaction. You can notify us free of charge via the Freephone number listed on our website [Redacted]. If an unauthorised payment is made from the Account, we will, subject to 6.3 & 6.4 below, refund the 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 the Account without further reference to you.

6.3 Where any unauthorised Cardholder Transactions have resulted from the loss, theft or misappropriation of the Card or PIN, 3D Secure Passcode or other Security Credentials, and the Customer is not a Microenterprise, the Customer will be fully liable for any such unauthorised Cardholder Transactions which occurred before such loss, theft or misappropriation was reported to the Bank. If you use your Card as a Microenterprise, you are liable for only €50 in unauthorised transactions carried out on the Account before you reported the issue, unless 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 Notwithstanding 6.3 above, where any such unauthorised Cardholder Transactions arise as a result of any fraud or gross negligence on the part of the Cardholder, the Cardholder shall be liable for the full amount of such unauthorised Cardholder Transactions.

/Cont'd...

6.5 Other than in the case of any fraud or gross negligence on the part of the Cardholder, the Cardholder shall not be liable for any transactions carried out after the Cardholder has notified the Bank of the loss, theft or misappropriation of the Card PIN, 3D Secure Passcode or other Security Credentials.

6.6 In the event we suspect or detect any fraud or unauthorised activity on the 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 the Account and/or any Card issued on the Account and will advise you and/or the relevant Cardholder of the block and how it may be removed.

I note that Regulation 97 of the 2018 Regulations, deals with a “payment service provider’s liability for unauthorised payment transactions” as follows:-

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:

98. (1) Notwithstanding Regulation 97 and subject to paragraph (3), a payer shall bear the losses relating to any unauthorised payment transactions, up to a maximum of €50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.

(2) Paragraph (1) shall not apply where—

- (a) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, except where the payer has acted fraudulently, or
- (b) the loss was caused by an act or omission of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced.

(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.

Regulation 96 (4) provides:

(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.

It is clear that the 2018 Regulations state that where a payment transaction is not authorised, the payment service provider shall refund the amount of the unauthorised payment transactions "immediately" except where the payers payment service provider has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing. In this instance, there is no allegation that the Complainant engaged fraudulently.

The Provider submits that the Complainant's security information coming into the possession of a third party must have been due to gross negligence such that the Complainant should bear all of the losses incurred as a result of the unauthorised payment transaction. The Provider, however, has offered no supporting evidence to show fraud or gross negligence on the part of the Complainant, as required by Regulation 96(4).

The Provider was asked by this Office whether it believes that the transaction was due to gross negligence or fraud of the Complainant in not fulfilling its obligations under Regulation 93 of the 2018 Regulations. The Provider has not alleged fraud but has stated that if the Complainant did not carry out this transaction, then the only other explanation is that it allowed or "through negligence" enabled the security information to be shared with another party who was not authorised or entitled to have such information.

The Provider submits that the Complainant failed through gross negligence to fulfil its obligations under the Regulations because it failed to keep the card and security credentials safe as required not only by the Regulations but also by the framework contract. The Provider states that it does not rely on the use of the Complainant's debit card in and of itself but rather that the PIN was used for the disputed transaction and the Provider submits that gross negligence is clearly evident from the facts of the situation.

The Provider submits that when the Complainant telephoned the Provider to report the unauthorised transaction, it advised that it only authorised one transaction in the sum of €100. The Provider says that the fact that none of the transactions across all the Complainant's Principal's cards used, match that amount, demonstrates that the Complainant cannot speak to what exactly transpired in the bar on the relevant date. The Provider also expressly states that it cannot speak to what exactly transpired but it submits that the Complainant's Principal ought to have noticed that cards were missing, when he went to pay for a taxi he had taken to his accommodation and stopped at an ATM to pay the fare.

The Provider says that when the Complainant's Principal took money out of the ATM, he should have realised that something was wrong and in any event, he ought to have noticed before the afternoon of the 21st.

/Cont'd...

Whilst the Provider accepts that the Complainant still had the debit card associated with the current account, which is the subject of this complaint, when its Principal phoned the Provider on 21 September 2019, the loss of the Complainant's Principal's personal/business debit card evidences a carelessness and a failure to keep his cards safe, in accordance with the framework contract.

The Provider goes on to highlight that the Complainant's Principal uses a single PIN for all of his debit cards, but it concedes that neither the framework contract nor the terms and conditions governing the account expressly state that a cardholder cannot use the same safety credentials for different cards. The Provider also states that while it cannot speak to what exactly transpired in the bar, the Complainant's Principal submits that it was possible for the PIN to have been observed by a person "shoulder surfing. The Provider goes on to state that if somebody was allowed to engage in such activity then this does not accord with the Complainant's contractual requirement to take the "greatest possible care". The Provider does not however, assert that this amounts to gross negligence.

The 2018 Regulations mandate that the Provider must provide "supporting evidence" to establish gross negligence on the part of the Complainant. The Provider's position in this matter is that if the Complainant did not carry out the disputed transaction, then the security information falling into the hands of a third party could only have been through gross negligence. I don't accept this.

This Office cannot rely on the Provider's assumption of gross negligence, in the absence of supporting evidence to establish gross negligence. The Provider has been unable to provide this Office with evidence that in my opinion supports a finding of gross negligence on the part of the Complainant.

Indeed, the Provider ultimately suggests that the Complainant, through its Principal, has demonstrated "carelessness", but I am satisfied that the Provider's obligation to refund the Complainant the amount of the transaction, is not measured by reference to carelessness, but rather by reference to fraud and gross negligence.

I am conscious that the Supreme Court considered the concept of 'gross negligence' in the decision in *ICDL Saudi Arabia v European Computer Driving Licence Foundation Ltd* [2012] 3 IR 327. In approving the High Court decision, a majority of the Supreme Court held that the appropriate test for gross negligence was a

'degree of negligence where whatever duty of care may be involved has not been met by a significant margin.'

Accordingly, the issue is whether the Provider was entitled to form the opinion that the Complainant's conduct amounted to 'gross negligence', in applying the significant margin test referred to above. On the basis of the evidence available, I don't accept that the Provider was entitled to take that view.

/Cont'd...

I am satisfied that Regulation 98 of the 2018 Regulations applies and the Complainant must bear the losses relating to any unauthorised payment transactions up to a maximum of €50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.

Accordingly, on the basis of the provisions of the 2018 Regulations and in the absence of evidence of gross negligence on the part of the Complainant, I consider it appropriate to uphold this complaint and to direct the Provider to refund an amount of €500 to the Complainant Company.

It should be noted in that regard that whilst the Provider was entitled to deduct €50 in accordance with the 2018 Regulations, I am satisfied that the Provider failed to meet its obligation to refund the Complainant Company “immediately” upon being notified that the transaction had not been authorised.

For that reason, I take the view that the Provider should make an additional compensatory payment to the Complainant Company in the sum of €50, to mark the delay which has ensued in the Complainant being refunded the amount in question, and taking account of that additional payment which is in the same amount as the Provider was entitled to deduct, the amount that falls to be repaid to the Complainant Company’s account is €500.


Accordingly, for the reasons outlined above, I am satisfied that this complaint should be upheld.

Conclusion

- My Decision pursuant to **Section 60(1)** of the **Financial Services and Pensions Ombudsman Act 2017**, is that this complaint is upheld on the grounds prescribed in **Section 60(2)(a)**.
- Pursuant to **Section 60(4) and Section 60 (6)** of the **Financial Services and Pensions Ombudsman Act 2017**, I direct the Respondent Provider to rectify the conduct complained of by reimbursing the Complainant the full amount of the transaction at issue in the amount of €500, taking account of the compensatory redress explained above, such monies to be paid to the account from which the monies at issue were debited in September 2019. I also direct that interest is to be paid by the Provider on the said payment directed, at the rate referred to in **Section 22** of the **Courts Act 1981**, if the amount is not paid to the said account, within a period of 25 days from today.
- The Provider is also required to comply with **Section 60(8)(b)** of the **Financial Services and Pensions Ombudsman Act 2017**.

/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
DEPUTY FINANCIAL SERVICES AND PENSIONS OMBUDSMAN**

24 June 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.