



<b><u>Decision Ref:</u></b>	2020-0329
<b><u>Sector:</u></b>	Banking
<b><u>Product / Service:</u></b>	Current Account
<b><u>Conduct(s) complained of:</u></b>	Disputed transactions Handling of fraudulent transactions
<b><u>Outcome:</u></b>	Rejected

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

The Complainant is a personal and business customer of the Provider. He has been issued with three cards connected to accounts with the Provider – a personal debit card, a credit card and a business debit card. The complaint concerns the number of disputed transactions which took place on all three cards.

#### **The Complainant's Case**

The Complainant claims he was the victim of fraud in **October 2015** perpetrated while on holiday visiting a European Capital. The Complainant states that he was on a football trip and visited a bar in the capital He argues that he was there with a number of friends and wanted to pay for a round of drinks and food which totalled about €120. The Complainant states that he provided his credit card but was advised that it had been declined due to an invalid PIN. He then provided two other cards, one of which was a business debit card and the other of which was a personal debit card. After several attempts, the Complainant states that he was told that these were declined due to an invalid PIN. He says that he subsequently settled the bill in cash.

The Complainant argues that the amounts ultimately charged to his cards were totally out of character with his spending pattern. He states that there are a number of ATM withdrawals from the night which were not his. As he accepts that one cannot withdraw cash from an ATM without a card and PIN, he claims that there must be CCTV evidence to back up his assertion that the ATM transactions were not his. He states that he was in the bar in question from 11:30 PM to about 2:30 AM local time. The Complainant claims that there are transactions in the venue taking place after he left the venue, and wonders how this could happen.

The Complainant asserts that his business debit card went missing but he was in possession of his credit card and personal debit card. The argument is made that the card may have been cloned to make it seem like he was present at the bar, and his PIN taken by deception.

The Complainant states that the Provider has alleged that he was grossly negligent, when in fact he was the victim of a fraud by an unscrupulous merchant. The Complainant had no idea that such an amount of money was being charged at the time. The Complainant states that he contacted the Provider on 10 October 2015 and a complaint was made to the local police by phone. He also made a complaint to An Garda Síochána on his return to Ireland.

The Complainant's representative points out that under clause 6.3 of the Provider's personal debit card terms and conditions, the customer is liable for only €75 of unauthorised transactions carried out on the account before it was reported. The Complainant claims that the Provider has not commented on this aspect of the complaint. It is argued that the Complainant was acting as a consumer and he was on holidays. The Complainant points out that the Provider is citing gross negligence under clause 6.5 as the reason for refusing to make the refunds but he says that there is nothing in clause 6.3 that makes this term subject to clause 6.5.

The Complainant also indicates that in its letter dated **24 April 2017**, the Provider refers to an incident in 2013 which it claims was similar. The Complainant states that the Provider initially refused to settle the 2013 matter but eventually it was fully settled with interest on 4 April 2014. The Complainant was not grossly negligent in those other similar circumstances and he questions why the Provider is alleging gross negligence now. It is argued that the inconsistency in the Provider's actions is confusing and misleading and that the Complainant should be entitled to rely on the Provider's previous decision to give him protection.

In light of the size of the transactions which were considerably outside the normal range, the Complainant questions why the Provider did not place a 'stop' on the transactions. He also disputes that he engaged in grossly negligent behaviour. The Complainant argues that the incident in 2013 was settled and so he was led to believe that the Provider was there to protect against fraudulent behaviour. He argues that fraud is clearly possible notwithstanding the use of chip and PIN.

The Complainant is seeking a refund of €14,559.36 plus considerable interest.

### **The Provider's Case**

The Provider states that the Complainant received a text message from its security team on 10 October 2015 and contacted the Provider at that time. It states that during his discussions with the agent, the Complainant confirmed that he had used his chip and PIN security details on his credit card on more than one occasion, only to be informed by staff at the premises that the card was not working. The Provider states that its agent advised him to make a report to the local police as quickly as he could. On the call, the Provider states that the Complainant confirmed that he still had the credit card in his possession but that there was more activity on his other debit cards.

/Cont'd...

The Provider states that the credit card was not cancelled at the time as the Complainant had the card in his possession. It states that his call was then transferred to the debit card team to discuss the issue with those cards. The Provider is unable to locate a recording of this telephone call.

In a further call 3 days later, on 13 October 2015, the Provider states that the Complainant was advised that as the transactions were made using chip and PIN, that the case would not be recognised as fraud. The Provider states that the Complainant was transferred to customer service to be advised of the disputed transaction process and then transferred to the debit card section. The Provider states that the Complainant confirmed to the debit card team that he had the personal debit card in his possession but that the business debit card was missing. The cards were cancelled and the Complainant was advised that he should make a report to the Gardaí. The Provider states that the Complainant was advised that it could not be taken as a fraud case.

In another call on **15 October 2015**, the Provider again informed the Complainant that the transactions which are complained of could not be taken as fraud. In a further call on **16 October 2015**, the Complainant informed the agent that he had the same PIN for each card. He also confirmed that he did not check the amount being entered on the card terminal.

On **3 November 2015**, the Provider states that a liability letter was issued in respect of the business debit card and personal debit card which confirmed that the Provider was holding the Complainant liable for all transactions made on the accounts. A similar letter was sent in respect of the credit card dated **26 November 2015**.

At that point, the Complainant rang to complain in respect of the rejection letters received on **27 November 2015**. The Provider states that a telephone call was made to the Complainant to discuss the complaint and to ascertain what happened on the night of the disputed transactions. It states that a five-day acknowledgement letter was issued to the Complainant on 2 December 2015 and a 20 day letter issued on 26 January 2016, with the Provider's final response letter issuing on 23 February 2016. Following a further complaint to the local branch of 31 March 2016, a further letter was sent by the Provider dated 4 April 2016 advising that the Provider's final response letter of 23 December 2015 remained its position.

The Provider states that it is satisfied that the Complainant demonstrated gross negligence in its operation of his business debit card personal debit card and credit card while he was abroad in October 2015. The Provider argues that this was not an isolated incident as the Complainant had experienced a similar loss on his three accounts previously in the same country under the same circumstances in 2013. The Provider asserts that the Complainant failed in his duty of care in respect of all his accounts by failing to keep his cards and his security details safe as required and set out in the terms and conditions of all three accounts. Furthermore, the Provider argues that as this was the second time the same 'theft' occurred, the Complainant was or should have recognised the same tactics being used by the perpetrators of those transactions. The Provider also points out the number of transactions on each card at both point-of-sale terminals and ATM machines to obtain funds.

/Cont'd...

The Provider states that the Complainant has asserted that he left the establishment around 02.30 in the morning of 10 October 2015, but its records confirm that the attempts to obtain money from the three accounts started shortly after 23.37 on 9 October 2015 up until 04.51 on 10 October on his debit cards, and from 23.37 on 9 October 2015 up until 05.18 on 10 October 2015 on his credit card. The Provider states that all transactions attempted were made using Complainant's personal chip and PIN details and using the actual cards.

The Provider relies on the terms and conditions of the various bank accounts in support of its arguments. The Provider accepts that the transactions are subject to the European Communities (Payment Services) Regulations 2009 (**PSR 2009**).

The Provider states that the Complainant confirmed in a telephone call with it, that he attempted to make a transaction but was advised by the staff of the establishment that the PIN was coming back as incorrect. The Complainant re-entered in a number of times with a number of cards, which allowed the third party to take funds from the three accounts. The Provider states that records also confirm that on at least five occasions, the three cards were not in the Complainant's possession allowing the third parties to access funds from an ATM. The Provider states that the transactions took place from approximately 23.37 PM on 9 October and to 5:18 AM on 10 October 2015 (Irish time) using both the card terminal and an ATM machine to access the funds.

The Provider states that if it is accepted that someone carried out the transactions without the consent of the Complainant, they were carried out: (a) without his consent but (b) with the card details and the chip and PIN personal security details. The Provider does not believe this to be the case and remains of the view that the Complainant carried out the transactions complained of, as evidenced by the use of the actual cards in conjunction with the personal security credentials.

Without prejudice to this position, if the transactions were considered unauthorised, the Provider argues that the Complainant's personal and previous experiences renders his behaviour grossly negligent. The Provider argues that the Complainant had a previous claim against the Provider in respect of allegedly unauthorised transactions which arose in almost identical circumstances in the same country, in which a large sum of money was taken from three cards. The Provider argues that it is because of, and not despite, this previous incident that the Provider is refusing to refund the Complainant as he should have been actually aware of potentially fraudulent activities, having fallen foul of the same in the past.

The Provider argues that specific personal knowledge or experience can render the activities of one person grossly negligent even though those activities might not be considered grossly negligent carried out by different person. Taking account of the relevant prior experience of the Complainant, the Provider argues that the standard of care owed by the Complainant is now actually higher than previously applied.

### **The Complaint for Adjudication**

The complaint is that the Provider wrongfully refused to refund a series of transactions across three debit and credit cards belonging to the Complainant, which he maintains were fraudulent.

### **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 **8 September 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 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.

There are a number of the transaction that occurred on the Complainant's three cards (his credit card, his personal debit card and his business debit card) on the night of 9-10 October 2015, detailed as follows:

<b>Card Type</b>	<b>Date</b>	<b>Local Time</b>	<b>Amount €</b>	<b>Payment Type</b>	<b>Vendor</b>
Credit	09.10.15	12.37	1,173.28	Chip and PIN	Named Bar
Business Debit	10.10.15	02.05	356.55	Chip and PIN	ATM
Credit	10.10.15	02.09	1,173.28	Chip and PIN	Named Bar

/Cont'd...

Credit	10.10.15	02.42	2,335.05	Chip and PIN	Named Bar
Personal Debit	10.10.15	02.59	1,188.26	Chip and PIN	ATM
Personal Debit	10.10.15	03.16	475.40	Chip and PIN	Named Bar
Business Debit	10.10.15	04.51	130.45	Chip and PIN	ATM
Credit	10.10.15	04.58	1,173.28	Chip and PIN	Named Bar
Credit	10.10.15	05.25	521.57	Chip and PIN	ATM
Credit	10.10.15	06.04	117.35	Chip and PIN	ATM
Credit	10.10.15	06.18	1,173.28	Chip and PIN	Named Bar
Business Debit	10.10.15	-	1,188.26	Chip and PIN	Named Bar
Business Debit	10.10.15	-	1,188.26	Chip and PIN	Named Bar
Business Debit	10.10.15	-	2,364.87	Chip and PIN	Named Bar

It should be noted that all of the point-of-sale transactions took place in one single bar and all ATM transactions took place at one ATM. No explanation has been provided by the Provider as to why the times of the three remaining business debit card transactions have not been confirmed.

The Complainant's account of the transactions that occurred on 9 and 10 October 2015 is that he was in a bar in a European Capital and attempted to pay a food and drinks bill in the sum of approximately €120 using one of his cards. He has indicated that he input his PIN but was informed that the card was not working or that the PIN was incorrect. He thereafter tried to authorise the transaction using his PIN several times, and thereafter attempted to authorise the transaction using his other two cards, but was repeatedly informed that the PIN was incorrect. He says that ultimately, he paid the bill in cash.

The Complainant states that he was in the bar in question from approximately 11:30 PM to 2:30 AM and has no knowledge of any other transactions on his card. The Complainant states that the next morning, he was still in possession of his credit card and personal debit card but that his business debit card was missing. The Complainant has not provided any details as to how and when the business debit card may have been stolen or mislaid.

During a call with on 10 October 2015 (a transcript of which has been provided in evidence) the Complainant telephoned the Provider in response to a text message alerting him to suspicious activity on his credit card. The Complainant confirmed that he had attempted to use the card in question the previous evening and that he had the card in his possession. He questioned how many other transactions there had been and indicated that he had "*receipts here for . . . other amounts . . . because he's tried to put it through again and again*".

/Cont'd...

The Complainant expressed shock at the number of transactions identified by the representative but the representative informed him that all were made with his chip and PIN. The Complainant stated that he had been told that his card was not working and so he had put his PIN in again and again. He was advised to go the police station. The Complainant also indicated that he had *“the receipt here for [his] debit card as well”* and an attempt was made to transfer him to the debit card security team.

During another call on 13 October 2015 (a transcript of which has been provided in evidence) the Complainant confirmed that his credit card was still in his possession. The Provider’s representative informed him that a number of transactions had been made with his actual card and with his PIN. He was advised to contact the Gardaí.

During a call on 15 October 2020 (a transcript of which has been provided in evidence) the Complainant stated that his business debit card was missing when he awoke on the morning of 10 October 2015, but he was in possession of his personal debit card and his credit card. The Provider’s representative informed him that all transactions were made using his physical card and PIN. The Complainant stated that no one else was aware of his PIN, and he did not keep the PIN with his cards. The Complainant confirmed that his PIN was the same across all three cards. He accepted that it was possible that someone could have seen him type in the PIN but stated that he always covers his PIN.

During a call on 16 October 2015 (a transcript of which has been provided in evidence) the Complainant denied having used his credit card at the ATM at the bar in question. He suggested that perhaps the staff members at the bar took the opportunity to withdraw funds from his cards at that on-site ATM, while he was attempting to pay his bill and was being told that the PIN was incorrect. The Complainant stated that the staff left the counter with the card for a moment and he assumed they were simply putting it into the machine at the time. He again confirmed that the PIN was identical across all three cards. On another call on the same date, in respect of his business debit card, the Complainant explained that the teller told him that the PIN was incorrect and not the machine itself and confirmed that the teller gave him back the card.

In a recorded call with a customer complaint agent of the Provider on 26 November 2015, the Complainant asserted that his business debit card was taken on the night in question but he remained in possession of his credit card and personal debit card. The agent confirmed that each of the Complainant’s physical cards were used in each transaction as the actual chips were verified, in addition to the PIN associated with each card. In a further call on 27 November 2015 with the same agent, the Complainant stated that he arrived at the bar shortly after 11.00 pm and left around 02.30 am.

The Complainant was not sure of the exact amount of the bill entered by the vendor at the card terminal, but indicated that he concealed the PIN with his wallet in the customary manner. He claims that he was repeatedly informed by the merchant that the PIN was incorrect so he tried to complete the transaction on multiple times and with all three cards. He confirmed that he had the same PIN on all three cards.

/Cont’d...

The difficulty with the Complainant's account of what occurred on the night in question is that it does not correlate with the records submitted by the Provider. The Complainant contends that perhaps each of the transactions that he was told not been approved, were in fact authenticated. This cannot explain the transactions in question as this hypothesis would require that all the transactions occurred around the same time, while the Provider's records indicate that the transactions took place over a six-hour period.

The Complainant has indicated that he left the bar in question at approximately 2:30 AM and has not indicated that he went anywhere else on the night in question. He has further confirmed that two of the three cards were in his possession the following morning. All three cards, however, were utilised in the bar and/or at the ATM between 02.30 AM and 6:18 AM on the night in question.

The Complainant has raised a query as to whether his cards may have been cloned or skimmed in some way, but the Provider has confirmed that each transaction was carried out by the Complainant's actual cards, using the chip provided to him and that each transaction was authenticated using the Complainant's PIN. It is difficult to understand, therefore, how two of the Complainant's cards were in his possession the following morning when he left the bar in question at 02.30 AM, and yet all 3 cards were used between 02.30 and 06.18 AM. No further information has been provided in respect of the multiple receipts for his credit card and debit card referred to by the Complainant during his initial call with the Provider on 10 October 2015.

If there was fraudulent activity on the night in question, I take the view that there must be factors involved that have not been identified by the Complainant, such as a third party having been given use of his cards on the night in question, in conjunction with the PIN. In all of the circumstances and based on the information made available, I cannot criticise the Provider for forming the view that the transactions in question – which had been duly authenticated using the Complainant's physical cards and the associated PINs – were properly authenticated.

Furthermore, the Provider has argued that if the transactions were not authenticated and there was third-party fraud, the Complainant acted with gross negligence such that he is not entitled to a refund under the relevant terms and conditions of the card in question.

The relevant terms and conditions of the Complainant's personal debit card are as follows:

*3.2 You must keep the PIN . . . secret, memorise them and take the greatest possible care to prevent anyone knowing them or using them fraudulently or without your permission.*

...

*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.*

...

*4.2 You must make sure that a card transaction including the amount is correct before you enter your PIN...*

...

/Cont'd...



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

...

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 . . . became available to the finder or thief or someone else had access to the card . . .*

The relevant terms and conditions of the Complainant's business debit card are essentially identical as regards clauses 3.2, 3.2, and 4.3 above. Clause 6.3 of the terms provides that:

*. . . 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.*

Clause 13 of the relevant terms and conditions of the Complainant's credit card are as follows:

- (c) In the event of an unauthorised transaction 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 . . . and where such loss, theft or misappropriation was reported to the bank without undue delay you will be liable for such unauthorised transactions up to a maximum of €75.*
- (e) Where any unauthorised transactions arise as result of any fraud by you, or because you failed intentionally, or because of gross negligence on your part, to fulfil the obligations under these conditions of use, you shall be liable for the full amount of such unauthorised transactions.*

The credit card conditions of use contain comparable obligations to keep the PIN a secret; to take all reasonable precautions to prevent anyone else from knowing or using it; to protect the credit card; to take all reasonable precautions to ensure that credit card is not lost, mislaid or stolen; and to ensure the accuracy of all payment orders.

In case of all three cards therefore, the applicable terms and conditions obliged the Complainant to keep his card and associated PIN secret, to take all reasonable precautions to ensure their safety, and to ensure the accuracy of all payment orders. Furthermore, the terms and conditions provided that he would not be refunded for any unauthorised transactions arising because of gross negligence on his part, in fulfilling the obligations of use of each card.

It is accepted by the Provider that the disputed transactions were subject to the European Communities (Payment Services) Regulations 2009 (**PSR 2009**). These regulations provide for similar obligations on the Complainant as those set out in the terms and conditions set out above. Under Regulation 73(1), if a payment service user (the Complainant) denies having authorised an executed payment transaction, it is for the payment service provider concerned (the Provider) to prove that the transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other error or failure. It has been confirmed that the transaction was authenticated under the terms and conditions applying to the account.

Regulation 73(2), however, provides that:

*'the use of a payment instrument recorded by the payment service Provider is not in itself necessarily sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or intentionally or failed, because he or she acted with gross negligence, to fulfil one or more of his or her obligations under Regulation 70' where the customer has denied having authorised the transaction.'*

While a customer's liability for an unauthorised transition is generally limited to €75 where a payer's debit or credit card has been lost or stolen under Regulation 75(1), Regulation 75(2) PSR 2009 states that:

*'A payer shall bear the losses relating to an unauthorised payment transaction if he or she incurred them by acting fraudulently or by failing, intentionally or by acting with gross negligence, to fulfil one or more of his obligations under Regulation 70.'*

The obligations of payment service users (the Complainant in the present case) in relation to payment instruments as stated in Regulation 70 are as follows:

*'(1) The obligations of a payment service user entitled to use a payment instrument are—*

- (a) of using the payment instrument in accordance with the terms governing its issue and use, and*
- (b) of notifying the payment service Provider that issued the instrument, or an entity specified by that payment service Provider, without undue delay on becoming aware of the loss, theft or misappropriation of the payment instrument or its unauthorised use.*

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

As set out above, the Complainant in the present case is contractually obliged to keep the cards and their security feature safe.

/Cont'd...

The term 'gross negligence' is not defined in either the PSR 2009 or in the parent Directive (Directive 2007/64/EC). Recital 33 of Directive 2007/64/EC provides:

*'In order to assess possible negligence by the payment service user, account should be taken of all the circumstances. The evidence and degree of alleged negligence should be evaluated according to national law. Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer should be considered null and void.'*

The Irish 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 I have to examine the Complainant's conduct here to determine if the Complainant has acted with 'gross negligence' by applying the significant margin test referred to above.

As set out above, the version of events of the night of 9 - 10 October 2015 as submitted by the Complainant does not correlate with the records submitted by the Provider. The Complainant has argued that he was present at the bar in question between 11.30 and 02.30 approximately, and yet the point of sale transactions and ATM transactions in question continued for four hours after that point. Furthermore, the Provider has indicated that there was no question of the card being cloned and that the Complainant's actual cards were utilised in the transactions. The Complainant admits that two of the cards were in his possession the following morning. In addition, all transactions were authorised using the Complainant's PIN and across a six-hour period.

Although it is unclear to me how exactly the Complainant maintains that the third party could have discovered his PIN, since he says he covered the PIN insertion with his wallet, the suggestion appears to be that the fraudulent party watched as he inputted his PIN on all three cards in the earlier transaction and possibly retained the information for later use. I am unclear as to how it is suggested however, that the third party accessed the relevant cards for the transactions in question.

The Provider has submitted an excerpt from a previous claim made by the Complainant in February 2014. The letter states as follows:

*"I fully believe the vendor "robbed me" of my money €6846.89 by getting my PIN number and skimming my card or by telling me that my PIN number was incorrect and my cards where (sic) declined but in fact my PIN numbers where (sic) correct and they just typed in the high amounts above in the local currency (specified) unknown to me."*

/Cont'd...

I accept the Provider's argument that specific personal knowledge or experience can act to render the activities of one person grossly negligent, which activities might not be considered grossly negligent carried out by different person. I am satisfied that such considerations apply here considering the similarity of the incidents in 2013 and 2015, whereby the Complainant has said that he has been the victim of fraud.

In my opinion, the Complainant ought to have been suspicious when an identical pattern of activity presented itself (i.e. that he repeatedly tried to enter his PIN on a number of different cards and he was told that the PIN was incorrect, when he ought to have known that the number was correct). The Provider has also indicated that the Complainant was informed at the time of the original incident in 2013/2014 that it was unsafe for him to have an identical PIN number for each of the three cards. This has not been refuted by the Complainant. Despite the fact that this warning had been given, the Complainant continued to have an identical PIN across all three cards at the time of the incident in October 2015. Furthermore, in order for the transactions in question to have taken place, the Complainant had to have parted possession with all three of his cards over a considerable period of time and further to have allowed a third party access to his PIN (knowingly or unknowingly).

In light of these considerations and bearing in mind the specific personal experience of the Complainant from the 2013 incident, I accept the submissions of Provider that it was entitled to consider his behaviour to have been grossly negligent in all circumstances, to the extent that he was not entitled to any refund in respect of the disputed transactions.

In those circumstances, I am of the view that the Provider was entitled to form the opinion that the disputed transactions in question were properly authenticated based on the records, when compared to the Complainant's account of the night in question. I am also satisfied that even if the transactions were not authenticated by him, the Provider was entitled to take the view that the Complainant acted with gross negligence in respect of the disputed transactions. In either case, he is not entitled to a refund from the Provider in respect of the disputed transactions, either under the terms and conditions of the relevant cards or the terms of PSR 2009, and accordingly, I am unable to uphold the complaint.

### **Conclusion**

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

2 October 2020

/Cont'd...

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.

