



<b><u>Decision Ref:</u></b>	2022-0050
<b><u>Sector:</u></b>	Banking
<b><u>Product / Service:</u></b>	Debit Card
<b><u>Conduct(s) complained of:</u></b>	Handling of fraudulent transactions Dissatisfaction with customer service Disputed transactions
<b><u>Outcome:</u></b>	Upheld

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

This complaint concerns fourteen disputed transactions made on the Complainant's Visa Debit Card account which is held with the Provider.

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

The Complainant asserts that he was in a bar ("**Company A**") in a European Country on **10 August 2019** and that he made a single transaction for €400.00 (four hundred euros) on his Visa debit card but noticed on [date Redacted] **2019** that further transactions amounting to €11,450.00 (eleven thousand four hundred and fifty euros) had left his account. The Complainant submits the Provider wrongfully failed to reimburse him the monies and further that the Provider advised him incorrectly of the relevant reporting procedure leading to a delay in reporting.

The Provider has supplied the following list of transactions and the Complainant disputes transaction 2-15 from the below list.

<b>No.</b>	<b>Date</b>	<b>Time</b>	<b>Merchant</b>	<b>Amount €</b>	<b>Disputed</b>
1.	10.08.19	00:10	Company A	400	No
2.	10.08.19	00:36	Company A	500	Yes
3.	10.08.19	00:36	Company A	300	Yes

4.	10.08.19	00:36	Company A	1,000	Yes
5.	10.08.19	00:37	Company A	1,000	Yes
6.	10.08.19	00:37	Company A	1,000	Yes
7.	10.08.19	00:37	Company A	1,000	Yes
8.	10.08.19	00:37	Company A	1,000	Yes
9.	10.08.19	00:38	Company A	1,000	Yes
10.	10.08.19	00:38	Company A	1,000	Yes
11.	10.08.19	00:39	Company A	500	Yes
12.	10.08.19	00:39	Company A	2,000	Yes
13.	10.08.19	01:03	Company A	350	Yes
14.	10.08.19	01:57	Company A	400	Yes
15.	10.08.19	02:05	Company A	400	Yes
<b>TOTAL DISPUTED</b>				<b>€11,450</b>	

The Complainant submits, by letter dated **4 November 2019**, that:

*“While on holiday I went to a bar in [a European Country] and as a treat for myself, as [event redacted], I bought myself and some friends a bottle of Champagne that cost 400 euro. This was the only time I had used my card on the holiday and at no time was it not on my person during the holiday, expect to hand it over to the barman to pay for the champagne. When I got back from the holiday on the Monday, I went to order something online and my card kept getting refused so I checked my account with online banking and realised I had less than 60 euro in the account. There were 14 transactions from a company called [Company A] totalling 11,450 euro that was taken out of my account over a twenty-minute period without my permission. I called [Provider] immediately to see how this could have happened and what I needed to do to get my money back. I was told to cancel the card and to file a ‘Transaction Dispute Form’ for each of the transactions that were made without my knowledge and that I should get money back once this was done. This however turned out to be the wrong procedure to follow and after two weeks of going back and forth with the bank I was finally told that I actually had to file a statement to the Garda, then go through Card Security and that because the transactions were Chip & Pin the transaction dispute form was useless. So, I put in a report with [Location] Garda Station (Report Number xxxxxx277) and filed a report with Card Security. They got back to me and told me (see attached letter) that because it is impossible to clone a chip and pin card, a quick google in fact shows it is indeed quite possible, even though the card never left my wallet that I was at fault for the transactions and they would be rejecting my claim.”*

/Cont’d...

The Complainant submits that he made a report to the Garda Síochána and filed a report with the Provider's Card Security Department. He states that the Provider's Card Security Department responded saying that it would be rejecting his claim because it is impossible to clone a chip and PIN card. The Complainant disputes this.

The Complainant contends that it was not possible for him to report misuse of his card prior to the transactions being made and he asserts, by letter dated **4 November 2019**, that:

*"They also claimed in this letter that 'the transactions shown above were made prior to the misuse of the card being reported to [Provider]' how is this even possible, apparently you need to be a mystic to properly report fraud!"*

The Complainant also argues, by letter dated **4 November 2019**, that:

*"One question I have asked a million times is why was this not flagged as suspicious activity and why wasn't I contacted to let me know 11,450 euro was spent in twenty minutes. This was clearly suspicious as I have been with the bank since 2011 and have never spent close to that amount in a month let alone in the space of twenty minutes, I have never received a response to this question."*

The Complainant says that he authorised a single €400.00 (four hundred euros) transaction for a bottle of champagne and that all other transactions were unauthorised. He surmises that this may have been arising out of the cloning of his chip and pin card. The Complainant is dissatisfied with the Provider's advice regarding the correct reporting procedure and the Provider's failure to prevent the transactions as they were, the Complainant asserts, unusual banking activity. The Complainant wants a refund of the monies lost.

The Complainant states that when he returned home from his holiday he discovered, it appears on the **[Date Redacted] 2019**, that he had less than €60.00 (sixty euros) in his account. He submits that his account showed 14 transactions for [Company A] totalling €11,450.00 (eleven thousand four hundred and fifty euros). He states that this amount had been taken from his account within a 20 minute period and without his authorisation.

The Complainant submits that he called the Provider to query how this could have happened and to seek information about what he needed to do to get his funds back. He submits that the Provider told him to cancel the visa debit card and to file a *Transaction Dispute Form* for each of the transactions that were made without his knowledge and that he should get his funds back once this was done.

The Complainant submits that the Provider had informed him of the incorrect procedure to follow and that after 2 weeks passing, he says, he was told that he had to file a statement with the Garda Síochána, then go through its Card Security Department and that because the transactions were chip and PIN the Transactions Dispute Form was inadequate/not appropriate for the circumstances.

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

The Provider submits the debit card transactions logged a particular message which means that they were verified by a chip on the card, which cannot be cloned. The Provider accepts that the Complainant should have been referred by its agents, to the correct procedure and it has offered compensation to the Complainant in that regard.

The Provider submits that it is not obliged under the Regulations, or its Terms and Conditions to monitor the transactions on the Complainant's account. Additionally, the Provider says it has not been supplied with any report from the Gardaí.

The Provider submits that the fifteen transactions which occurred on **10 August 2019**, "*are all associated with Merchant Category Code 7273: '[Type Redacted] Services', and were authorised and executed using chip and PIN.*"

By letter dated **10 September 2019**, the Provider submits that:

*"We have completed an investigation into this report and have found that the above POS (Point of Sale) transactions shown above were made prior to the misuse of the card being reported to [Provider].. Point of Sale transactions can only be made when the card is used in conjunction with a personal identification number (P.I.N). In this instance, this transaction was carried out on your genuine Chip card in conjunction with your P.I. N. There is a contract in place between you and the [Provider], which governs the use of the Debit Card and as such the transactions are considered to be correctly authorised. As per the Terms & Conditions of the Debit Card, you are liable for these transactions."*

The Provider submits that:

*"Contrary to what has been stated by the Complainant, the Provider's records indicate that he did in fact use his card on other occasions during his holiday. At 9.58 p.m. on 9 August 2019, the Complainant authorised a transaction for €20.00 in [Company B], which transaction was associated with Merchant Category Code 5812: "Eating Places & Restaurants". The transactions in [Company A] were authorised*

/Cont'd...

*between 12.10 a.m. and 2.05 a.m. on 10 August 2019....All executed transactions on the night of 9/10 August 2019 were authorised using chip and PIN, meaning the Complainant's physical debit card was present, and his correct PIN was entered into the card terminal.*

*The Complainant theorises that his debit card was cloned when he authorised the transaction for €400.00 at 12.10 a.m. on 10 August 2019. The next transaction was executed at 12.36 a.m., and this transaction is disputed by the Complainant. To clarify, when a payment card is cloned, the information contained on the card's magnetic stripe is copied from the original card to a new, blank card. The magnetic stripe contains the card details including the CVV number. Where a chip card is concerned, a different CVV number is encrypted on the chip in the card, referred to as the iCVV number - this cannot be cloned. Each of the disputed transactions was associated with the correct iCVV number ("Integration circuit card read-CVV data reliable" - please see Response 3, above); the card was therefore not cloned. Furthermore, it would not have been plausible for even the magnetic stripe to have been cloned in the short period of time between 12.10 a.m. and 12.36 a.m. The Complainant's cloning theory is unfortunately without merit in the circumstances... The Provider's records cannot be falsified, and, contrary to what has been asserted by the Complainant, it is not possible to clone the chip in a debit card."*

Regarding the Complainant's assertion that the transactions should have been flagged as fraudulent, The Provider says that:

*"The Provider operates a fraud monitoring system incorporating a neural scoring engine in conjunction with rules and strategies. The neural score in conjunction with the rules is designed to highlight possible fraudulent activity which may be out of character on customers' accounts. It does so by analysing known frauds as well as information received from Visa and Mastercard. For security reasons, the Provider cannot provide any further detail than this, as to why the disputed transactions were not flagged, or why the Complainant received no notifications in respect of same. By way of general comment, the Provider respectfully submits that it was not obliged under the Regulations, or the Framework Contract, to monitor the transactions on the Complainant's account. Furthermore, all disputed transactions were considered correctly authorised within the terms of the Framework Contract."*

The Provider also contends that:

*"It is the Provider's understanding that no report was made to the police in the European country. No documentation has been furnished to the Provider in respect of any police report."*

/Cont'd...

Commenting on the phone call of **12 August 2019**, the Provider submits that:

*“If it is the case (as seems to be conceded by the Complainant) that the bar staff in [Company A] input the wrong sums to be debited into the card terminal, and that the Complainant authorised these amounts due to carelessness, then liability clearly lies with him in the circumstances.”*

Commenting on the phone call of **12 August 2019**, the Provider also submits that:

*“The purpose of a transaction dispute form is to lodge a dispute with the Provider's chargebacks department. The chargeback procedure can be engaged by the Provider to dispute and reverse certain card transactions, where the criteria set by Visa and Mastercard are satisfied. Unfortunately, chip and PIN transactions fall outside the scope of the chargeback scheme. It appears that, while this position was not explicitly stated by either of the Provider's agents during the course of the phone call of 12 August 2019, they were alive to the fact that the use of chip and PIN put the Complainant in a difficult position, and did make him aware of this. The Provider respectfully submits that, in the latter part of the phone call, the agent appears to be advising the chargeback procedure primarily as a method of investigating the nature of the disputed transactions, rather than advising it as a guaranteed avenue of resolution.”*

The Provider upholds the complaint in relation to the Complainant having been incorrectly advised that he could dispute these transactions. However, the Provider rejects the Complainant's assertion that the transactions in the amount of €11,450.00 (eleven thousand four hundred and fifty euros) should be refunded. The Provider stated there is a contract in place which governs the use of the debit card and says that the Complainant was liable for these transactions, as per the terms and conditions of the debit card. The Provider asserts that the Complainant will remain liable for the transactions, as they were carried out using his card and PIN and that he had confirmed that he had his card in his possession on the night.

### **The Complaint for Adjudication**

The complaint is that the Provider wrongfully and/or unreasonably failed to reimburse the Complainant in the amount of €11,450 for unauthorised transactions undertaken on his account ending 8143. The Complainant is also unhappy that the Provider gave him incorrect information in relation to its reporting procedure, which resulted in a delay of more than 2 weeks, before it correctly informed him of the procedure and before he could report his loss, in the correct manner.

/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 **17 January 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.

Recordings of three telephone calls have been supplied in evidence and have been reviewed. The Complainant called Provider Agent 1 on Monday **12 August 2019** (18.02) and said as follows:

*“Provider Agent 1: “were you out on the tenth, the night of the 9th, the early hours of the tenth.”*

*Complainant: “I wouldn't have been out that late, I would have been out until twelve or one maybe. That night I got a little too drunk and I had to go home - one of my mates had to take me home like.”*

...

*Provider Agent 1: “what's most likely to have happened is the staff there seem to have taken advantage and put in a much higher amount than you were expecting to pay for the drinks or whatever it was that you were paying for whilst you were out.”*

*Complainant: “yeah.”*

....

/Cont'd...

Provider Agent 1: *"what you would have to do in this situation is do what is called a transaction dispute....these transactions were done with the physical card and the pin."*

....

Complainant: *"so, what's the deal? Am I just [inaudible] here for the cash?"*

Provider Agent 1: *"what you'd have to do is a transaction dispute - now, I can pop you over to customer service and they can explain it a little better than me. Because they're chip and PIN transactions and you were in [Country], we wouldn't be able to take it on as fraud - you do have the card and everything in your possession and everything still. So if you hold the line there I'll pop you over to customer services there and they will talk you through the best way to get your money back on this transaction."*

*[Transfers Complainant to Provider Agent 2]*

Provider Agent 2: *"...I was just speaking to my colleague [Provider Agent 1] about your transactions and how we are going to help you hopefully go about disputing them and getting the money back for you if we can."*

...

Provider Agent 2: *"it's an awful lot of money to lose and I am hoping now that we can help you with that, I am sure we can.."*

....

Provider Agent 2: *"now, I'm not quite sure how successful it will be, because the transactions seem to be chip and PIN verified - so, someone had your card and had your PIN, which is kind of the unfortunate part here, but we'll definitely do our best for you. But get the forms in to us first of all and that will start the ball rolling. Now, I'll warn you: it's not going to be a quick process, it's not going to be over in a couple of days - it's going to take a number of weeks before this is resolved, I'd imagine."*

Complainant: *"yeah, yeah [inaudible]."*

Provider Agent 2: *"but get those forms into to us as soon as you can, and even if you're filling them out and you're a little unsure, just call this number again and we can talk you through it more. But it's more or less to look for the details of the transaction more so than anything else."*

The Complainant submitted 14 Transaction Dispute Forms (one of which says 1,000 instead of 400). I note that by letter dated **19 August 2019**, the Provider's Chargeback Department wrote to the Complainant and said as follows:

/Cont'd...



*“Having reviewed the information you have provided we regret to inform you, that in this case, under Visa Europe and MasterCard International Rules and Regulations, we have no dispute rights for Chip and Pin verified transaction(s). We would suggest you pursue the matter with the Merchant directly.”*

The Complainant asserts that *“I was told to cancel the card and to file a ‘Transaction Dispute Form’ for each of the transactions that were made without my knowledge and that I should get money back once this was done.”*

I am satisfied that the incorrect procedure was laid out to the Complainant and a number of misleading comments were made including Provider Agent 1 saying that *“they will talk you through the best way to get your money back on this transaction”* and Provider Agent 2 saying *“we are going to help you hopefully go about disputing them and getting the money back for you if we can”* and saying *“it’s an awful lot of money to lose and I am hoping now that we can help you with that, I am sure we can.”*

The Provider submits that it appears to be conceded by the Complainant that the bar staff at [Company A] input the wrong sums to be debited into the card terminal and that the Complainant authorised these amounts due to carelessness. I do not accept however, that this suggestion was conceded by the Complainant. It is certainly the case that during the telephone call of 12 August 2019, the Provider Agent suggested this as a potential explanation and the Complainant answered *“yeah”* but I do not accept that this was an affirmation on his part, that the Provider was correct in its surmising in that regard.

However, importantly, during the course of the [Date Redacted] 2019 telephone call, Provider Agent 2 said *“now, I’m not quite sure how successful it will be, because the transactions seem to be chip and PIN verified - so, someone had your card and had your PIN, which is kind of the unfortunate part here, but we’ll definitely do our best for you.”* I am satisfied that although the Complainant was told to engage in the incorrect internal procedure for investigating the disputed transactions and was given some inadvisable assurances by the Provider’s agents, this was qualified by other information. I am not satisfied that the Complainant was given a blanket guarantee that he would get his money back and I am satisfied that he was aware that the procedure he was engaging in, would not necessarily be successful, because the disputed transactions were chip and pin verified.

The Complainant called Provider Agent 3 on **23 August 2019** (12.15) as said as follows:

Provider Agent 3: *“...the establishment that is there is coming as [Company A]. Were you anywhere near that establishment or anything like that at the time.”*

/Cont’d...

Complainant: *"hold on two secs. Sorry about that, yeah, yeah I was, I think that was a nightclub that I was in, in [City]."*

...

Provider Agent 3: *"you were in this nightclub, obviously, can you remember the whole night? Is there at any stage [inaudible]."*

...

Complainant: *"yeah, like literally I can remember everything."*

...

Complainant: *"the only time they would have had it, is eh, your one did take it now for like I would say thirty seconds, you know when you put the card in and you put in your pin in and you give it back to them and they take out the receipt and they give it back to you, literally that was all it was."*

...

Complainant: *"...whatever that first transaction is, whatever time that is, that is when I would have been there, I would have been there for an hour or two and then I left."*

...

*"say about twelve till two."*

*"yeah, I would say so yeah."*

Provider Agent 3: *"and the card as you said wasn't out of your possession at any stage."*

Complainant: *"no it literally that was the only time it was out of my possession and I would have been watching them, you know. She would have just taken it and given it back to you."*

...

Provider Agent 3: *"... you said you didn't notice anyone around you at any stage that might have been looking over your shoulder or anything?"*

Complainant: *"I was literally up at a bar. There were people around me, yeah, but I wouldn't have noticed - it would have been a packed bar."*

/Cont'd...

Commenting on the phone call of **23 August 2019**, the Provider submits that:

*"The Provider respectfully submits that the Complainant's claim that he remembers the whole night of 9/10 August 2019 is somewhat at odds with the account given in his first phone call, namely that he had to be brought home by a friend because he was too drunk.*

*The Provider further submits that, between the records on its systems, and the accounts given by the Complainant, there are two possible scenarios likely to have occurred. The first is that the Complainant authorised all the disputed transactions, whether knowingly or not. The second is that a fraudster parted the Complainant with his debit card, discovered the Complainant's PIN, executed the disputed transactions, and returned the Complainant's debit card to him. As to how the fraudster might have become aware of the Complainant's PIN, the following interaction from the second phone call is informative:*

*Agent:... You said you didn't notice anyone around you at any stage that might have been looking over your shoulder or anything?*

*Complainant: I was literally up at a bar. There were people around me, yeah, but I wouldn't have noticed - it would have been a packed bar."*

In relation to the matter of whether the debit card could have been cloned, the Provider submits that:

*"Each of the disputed transactions has an associated transaction summary document which is automatically generated. On each such document related to the disputed transactions, the entry mode is stated to be 'Integration circuit card read-CVV data reliable'; the Provider can confirm that this means that the Complainant's physical debit card was used in respect of each transaction. Also on each such document, the cardholder identification method is stated to be 'Online PIN Use to identify an original transaction with PIN'; the Provider can confirm that this means that the correct PIN was entered into the card terminal in respect of each transaction."*

I have reviewed the fifteen Transaction Summaries furnished and all of them reference *"integration circuit card read-CVV data reliable."* I am satisfied that this is sufficient evidence that the transactions were verified by the physical debit card and that the chip and pin was utilised for these transactions. I also note that under "Merchant/Acquirer information", the *Merchant Group* says "risky purchase" and that the *Merchant Category Code* says "7273, [type redacted] Services".

/Cont'd...

The Provider relies on the **Terms and Conditions** for the Debit Card and the **Terms and Conditions** for the personal current account. The **Terms and Conditions** for Debit Cards are relied on by the Provider at clauses 3.0, 3.2, 3.4, 3.5, 3.6, 4.0, 4.1, 4.2, 5.0, 5.1, 5.2, 6.0, 6.3, 6.4, 6.5, 6.6, 9.2, 14.0 and 14.1 and these are as follows:

*“3.0 Protecting your Card, PIN and other Security Credentials*

....

*3.2 You must keep the PIN secret, memorise it and take the greatest possible care to prevent anyone knowing it or using it fraudulently or without your permission. You should never write down the PIN in a place where you also keep the Card or where it can be easily linked to your Card.*

*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 [Website provided]*

*3.6 You are responsible for your Card and you must ensure that you protect it in line with this clause 3.0. If you do not do so, you will be liable for any loss suffered as a result.*

....

*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.*

*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.*

...

*5.0 Paying a Retailer using Your Card*

*5.1 When using your Card for purchases in a retail outlet you may be asked to either enter your PIN or hold your Card against a Card reader depending on the payment terminal.*

*5.2 Chip & Pin Transactions*

*(i) For transactions which require a Card to be inserted into the POS terminal you will be generally prompted to input your PIN into the POS terminal.*

....

/Cont'd...

*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*

*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.*

....

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

- (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*

/Cont'd...

(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.*

(ix) *we have good reason to believe you do not wish to use your Card in future; you agree that we can assume you do not wish to use your Card in future if you do not use it for a continuous period of 90 days or more.*

#### *14.0 Disputes or Unauthorised Transactions*

....

*14.1 If there is a dispute about your Account or Card, you accept that the records kept by us or on our behalf are sufficient evidence of your Card's use. If a transaction is made using your Card with the PIN, the Card reader in a Contactless transaction or the 3D Secure Passcode, you agree that we can conclude that the transaction was made by you."*

The Provider also relies on clauses 6.2, 12.0, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.10, 23 and 23.4 of the **Terms and Conditions** of the Personal Current Account which provide as follows:

*"6.2 You can instruct us to carry out an Account transaction or give your consent (for example, a consent to allow us give you a service) by following the procedures we set out for you now or in future, for example:*

*(a) by using your Security Credentials;*

*(b) by using a Payment instrument;*

*(c) in writing (for example, by writing to a branch):*

*(d) verbally (as long as you follow our security procedures); or*

*(e) using 365 Phone.*

...

#### *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 website furnished].*

/Cont'd...

12.3 Our records of transactions may be kept on paper, microfilm, electronically or in other ways. You agree that if there is a dispute between you and us regarding a transaction that, in the absence of obvious error, these records are evidence of dealings in relation to your Account.

12.4 If payment is made from your Account that was not authorised by you 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 further 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.

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 any payments from it if:

...

(v) We have reason to suspect there is unauthorised or fraudulent activity on your Account even where we think you are innocent.”

The transactions at issue were subject to Council Directive 2015/2366/EC, the Payment Services Directive 2 (“PSD2”) which was introduced to Irish law by the **European Union (Payment Services) Regulations 2018** (the “Regulations”). The Provider relies on Regulations 76, 88, 93, 96 and 98 and Recital 72 of PSD2 and outlines the ways in which the **Terms and Conditions** for the Debit Card and the **Terms and Conditions** for the personal current account meet its obligations under the Regulations.

Regulation 76 (e) (“Information”) of the Regulations says as follows:

*“(e) on safeguards and corrective measures:*

*(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;”*

/Cont’d...



Regulation 98 says as follows:

*"Payer's liability for unauthorised payment transactions*

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.*"

[my underlining added for emphasis]

The Provider says that its **Terms and Conditions** of the Debit Card and **Terms and Conditions** of the current account meet the requirements of the Regulations.

*"Regulation 98 sets out at length the circumstances in which a payment service user will be liable for unauthorised transactions, e.g. through fraud or gross negligence on their part. Regulation 76(e)(iv) is satisfied by clause 6.5 of the Debit Card Terms and Conditions...*

*It is also satisfied by clause 12.6 of the Current Account Terms and Conditions."*

Having reviewed the Provider's submissions in this respect, I am satisfied that Regulation 76 has been applied in its **Terms and Conditions** of the Debit Card and **Terms and Conditions** of the current account.

/Cont'd...

Regulation 88 of the Regulations reads as follows:

*“Consent and withdrawal of consent*

*88. (1) A payment transaction is authorised by a payer only where the payer has given consent to execute the payment transaction.*

*(2) A payment transaction may be authorised by a payer either—*

*(a) prior to, or*

*(b) where agreed between the payer and the payment service provider, after, the execution of the payment transaction.*

*(3) Consent to execute a payment transaction or a series of payment transactions shall be given in the form agreed between the payer and the payment service provider concerned.*

*(4) Consent to execute a payment transaction may be given via a payee or a payment initiation service provider.*

*(5) Consent may be withdrawn by a payer until such time as the payment order concerned is irrevocable under Regulation 104.*

*(6) Consent to execute a series of payment transactions may be withdrawn by a payer, in which case a payment transaction scheduled to be executed after the date the consent is withdrawn shall be unauthorised.*

*(7) The procedure for giving consent shall be agreed between the payer and the payment service provider concerned.”*

The Provider submits that:

*“The Provider can confirm that the Framework Contract did provide a means for the provision of consent as required by Regulation 88. Clauses 4.1, 4.2, 5.1, 5.2 and 14.1 of the Debit Card Terms and Conditions all deal with the means of providing consent, as do clauses 6.2 and 12.3 of the Current Account Terms and Conditions. For the purposes of the present complaint, clauses 5.1 and 5.2 of the Debit Card Terms and Conditions are the most relevant.”*

Regulation 93 reads as follows:

*“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*

/Cont'd...

*(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.*

[Underlining added for emphasis]

The Provider submits that:

*“... the Complainant failed through gross negligence to fulfil his obligations under Regulation 93 of the Regulations, in that he failed to keep his card and security credentials safe as required under Regulation 93(1)(a) and (2)”:*

The Provider further submits that, *“in failing to keep his card and security credentials safe, the Complainant failed through gross negligence to fulfil his obligations under the Framework Contract, which are set out in clauses 3.2, 2.4 and 3.6 of the Debit Card Terms and Conditions.”*

Regulation 96 of the Regulations provides 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."*

[Underlining added for emphasis]

The Provider submits that:

*"Paragraphs (3) and (4) of Regulation 96 provide that, where a payment service provider alleges gross negligence on the part of a payment service user, the use of a payment instrument simpliciter will not be sufficient evidence to support the allegation, with additional evidence being required.*

*For the avoidance of doubt, the Provider does not rely on the use of the Complainant's debit card in and of itself to support the allegation of gross negligence; as is set out at Response 3, above, the Provider's systems demonstrate that the Complainant's PIN was used for each of the disputed transactions. Furthermore, the Provider submits that gross negligence is clearly evident from the facts of the case."*

Furthermore, the Provider relies on Regulation 98 as cited above:

*"Regulation 97 of the Regulations sets out the general scheme whereby payment service providers will be liable for unauthorised transactions, and Regulation 98 sets out the circumstances in which payment service users will be liable for unauthorised transactions. In the context of the present complaint, the Provider relies on Regulation 98(3)(b) for not providing a refund."*

Regulation 98(3)(b) provides as follows:

*"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- ...*

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

/Cont'd...

The Provider submits that:

*“Gross negligence’ remains undefined in the 2018 Regulations or in PSD2; however, Recital 72 of PSD2 states as follows:*

*‘In order to assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties.’”*

[Underlining added for emphasis]

I note that Recital 72 of PSD2 has *not* been adopted by the Regulations. The Provider however 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 case, 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.”* The Provider submits and I accept that the significant margin test *“remains the test for gross negligence in this jurisdiction.”*

The Provider submits in relation to whether the Complainant’s conduct meets the threshold for gross negligence that:

*“taken individually, the points outlined above might not of themselves meet the high threshold for gross negligence. However, when taken together, they evidence a pattern of carelessness, the totality of which demonstrates a clear breach of the terms of the Framework Contract, and a breach of the duty of care owed by a significant margin. The Provider therefore respectfully submits that the Complainant was grossly negligent for the reasons set out above.”*

I am satisfied that the test that the Provider must meet pursuant to the Regulations to show gross negligence on the part of the Complainant in failing to meet his obligations pursuant to Regulation 93, is the **“significant margin”** test referred to by the Supreme Court. The Provider must establish gross negligence by the Complainant in his use of the payment instrument.

/Cont’d...

I accept, in that regard, that the Provider has furnished evidence of negligence on the part of the Complainant. In particular I note that the Complainant says that he

*“bought myself and some friends a bottle of Champagne that cost 400 euro”, and that “that night I got a little too drunk and I had to go home - one of my mates had to take me home like.”*

He later submitted that he remembers everything about the night, but given the 2 opposing versions of events, it is difficult to accept the reliability of the Complainant’s recollection. Indeed, in the Complainant’s email submission of November 2019, he refers to handing over his card to “the barman”. During his phonecall however, on 23 August 2019, he said that *“your one did take it now for like, I would say 30 seconds...she would have just taken it and given it back to you.”* These accounts of what happened appear to be in conflict and indeed, although the Complainant said that he did not use his debit card in any other location whilst abroad, in fact he used it that very night, before attending the nightclub.

The Complainant agrees that he entered his pin at the bar and says his card was never out of his possession. He also notes that *“I was literally up at a bar. There were people around me, yeah, but I wouldn't have noticed - it would have been a packed bar.”* Given that this was the Complainant’s first transaction at the bar, it was incumbent on him to protect his PIN, including paying reasonable attention to those people who were around him in close proximity.

I take the view on the basis of this evidence that the Provider was entitled to conclude that the Complainant had no reliable recollection of the events of the evening in question. Whilst on one hand, the Complainant said that he was in the nightclub for about an hour, and later said he had been present at the nightclub between approximately 12 midnight and 2 am, he was also clear that he had to be escorted home by his friends, having drunk too much to be able to cater to himself, which suggests to me that he is unlikely to have noted what time he left the nightclub. All of these details are such that I accept that the Provider was entitled to conclude that the Complainant was indeed negligent, in protecting the security of his card on the night in question.

Whatever the explanation for these transactions however, I do not accept, on the basis of the evidence made available, that the Provider has demonstrated evidence of gross negligence on the part of the Complainant, as required by Regulation 96 (4).

In those circumstances, in the absence of evidence that the Complainant was grossly negligent, I am satisfied that the Provider has an obligation pursuant to the Payment Services Regulations to refund those transactions 2 – 15 set out in the table above.

/Cont’d...

In relation to whether or not the Provider should have flagged the activity as suspicious, I am satisfied that it would have been helpful if the Provider had blocked the card, in the face of these repeated transactions of significant value, in close succession, but I accept that there is no affirmative obligation on the Provider to monitor every transaction. To provide further clarity regarding these matters, I wrote to the Provider on **27 September 2021** raising a number of queries regarding the technical details apparent from the transaction summary documentation, which the Provider clarified by way of letter dated **22 October 2021**.

I also made clear to the Provider that this Office was unclear as to why the various details of the transactions in question did not trigger a response from the Provider which ought to have blocked at least some of the transactions which have been raised in this complaint, and I asked for the Provider's observations in that regard. The Provider in that respect advised that it could put the matter no further than it had previously (when it had advised that for security reasons it cannot provide any further details as to why the disputed transactions were not flagged, or why the Complainant received no notifications in respect of those transactions).

I am conscious that it is usual for financial service providers to have a certain level of monitoring of customer transactions in order to suitably flag those which may have high risk indicators, though I accept that there is no positive obligation on a provider to do so and, rather, it is more a matter of common practice by such financial service providers. I note that, in this instance, the Provider did not identify the Complainant's transactions in that manner or seek to block the card from any other transactions pending communication with the Complainant.

In recent times the Provider has made a goodwill offer to the Complainant in the sum of €1,000, on the basis that some of the information supplied to this Office may have been misleading or confusing to him. This settlement offer was declined by the Complainant.

In any event, given the absence of evidence of gross negligence made available by the Provider, (albeit that I accept that the Complainant was guilty of some level of negligence on the night in question) I am satisfied that the Provider was obliged pursuant to *Regulation 97(1)* of the *Payment Services Regulations 2018* to refund the Complainant the amount of the unauthorised payment transactions set out above at Transactions 2 – 15.

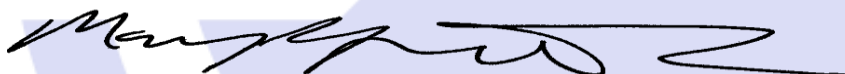
Accordingly, on the basis of the evidence available, I take the view that this complaint should be upheld.

/Cont'd...

## 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 make a payment to the Complainant in the sum of **€12,450** (twelve thousand four hundred and fifty Euro) to include the amount of the disputed transactions of €11,450, together with an additional compensatory payment of €1,000 in recognition of the Provider's failure to comply with its obligations under **Regulation 97(1)** of the **Payment Services Regulations 2018**, to make that refund to the Complainant immediately, and in recognition of the inconvenience thereby caused to the Complainant. I direct the Provider to make this payment to an account of the Complainant's choosing, within a period of 35 days of the nomination of account details by the Complainant to the Provider. I also direct that interest is to be paid by the Provider on the said compensatory payment, at the rate referred to in **Section 22** of the **Courts Act 1981**, if the amount is not paid to the said account, within that period.
- The Provider is also required to comply with **Section 60(8)(b)** of the **Financial Services and Pensions Ombudsman Act 2017**.

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)

8 February 2022

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.