An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

Decision Ref:	2021-0475
Sector:	Banking
Product / Service:	Debit Card
Conduct(s) complained of:	Handling of fraudulent transactions Dissatisfaction with customer service Unauthorised withdrawals
Outcome:	Rejected

LEGALLY BINDING DECISION OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

The complaint concerns a number of disputed transactions that were made on the Complainant's account, by way of point of sale terminal with PIN confirmation and at an ATM.

The Complainant's Case

The Complainant was travelling in a European City and he says that having arrived to his hostel at about quarter after midnight on Wednesday 15 January 2020, he and his friend dropped their bags and went to a local pub/club. The Complainant says that he consumed a complimentary drink upon entering the club and submits that, following this drink, he has "*little or no memory of what transpired that night*".

The Complainant notes that he does recall bar staff telling him that the PIN for his debit card had not been accepted. He says that over the course of the next 70 minutes, 17 transactions were attempted with his debit card. Five of those transactions were successful, and a total of more than €2,000 was taken from his account.

The Complainant says he woke at 4.10PM later that day with heavy limbs, and feeling very tired. He realised that money had been taken from his account and he contacted the Provider to inform it that the transactions were not authorised, and to seek advice. The Complainant then attended twice at a local police station to report the incident, but no English-speaking officer was available on either occasion.

On Friday **17 January 2020**, upon returning to Ireland, the Complainant emailed the police station to report the incident. He did not receive a reply.
During a phone call between the Provider and Complainant on **15 January 2020**, the Provider noted that a temporary hold had been placed on the Complainant's card at 00:50, after an attempted transaction of €692.05 (six hundred and ninety-two Euro and five Cent). It submitted that a text message had been sent to the Complainant to seek confirmation that the transaction was genuine, and the Complainant had confirmed the transaction via text.

In addition, the Provider has pointed to the fact that when this information was put to the Complainant over the phone he replied "*yeah*". However, in his complaint, the Complainant submits that he did not realise that this text had been received, or that an authorising text had been sent from his phone, until after he returned to Ireland:

> "*This was to confirm that the bank probably did send texts but NOT for me to authorise the transactions! and had no idea that these were already on my phone and replied to until 1 week later when the bank said this on their letter response*…"

During the same phone call, the Complainant was asked "*was that yourself*" in relation to the ATM transactions, and the Complainant responded: "*an ATM, yeah, that was me*". The Complainant submits in an email to this office of **9 November 2020,** that he had interpreted the Provider's question as asking whether that amount had been taken from his account. He submits that he did not carry out the ATM transactions or authorise any person to do so.

Insofar as the Provider has referred to contradictions between the Complainant's account of the night in question, and the account given by the Complainant's father, the Complainant noted in his email of **9 November 2020** that:

> *"I can confirm that the early part of the evening I do recollect using my card for a round of drinks, but as the night progressed, very quickly having no recollection or recognise (sic) these 16 attempts on my card or authorisation by phone text messages, which is what I told my father, and what I suspected happened to also (sic) the card team section of the bank the following day Jan 15th as per audio file."*

The Provider submits that the Complainant was grossly negligent on the night in question. The Complainant says, in an email of **9 November 2020**, that:

> *"At the very least to say, I am very disappointed at the provider's response in that some ways it infers a level of negligence or stupidity on my behalf in regards to protecting my banking details, which could not be further from the truth when it concerns my savings and I do "take the best possible care" to protect my card and its credentials from other parties. This was beyond my control for reasons aforementioned regarding the night in question."*

The Complainant submitted in an email to this office on **1 August 2020** that he was "*obviously involuntarily incapacitated*" during the incident. The Complainant acknowledges that he told the Provider that his debit card was in his possession at all times; however, he now realises that the perpetrator had control of his card and his phone.

/Cont'd…

The Complainant submits that the security procedures taken by the Provider were insufficient. He notes that suspicion should have been raised by the level of spending and the short period in which it took place. Further, he submits that the text authorisation was an inadequate means of verification and that a phone call would have been suitable.

The Provider's Case

The Provider submits that the first attempted transaction made on the Complainant's debit card was at 00:50:35 on **15 January 2020**, for €692.05 (six hundred and ninety-two Euro and five Cent). It says that a security alert was placed on the Complainant's card as a result of that attempt, and the transaction was declined. A temporary hold was placed on the card at 00:50, and a text message was sent to the Complainant seeking to confirm whether the transaction was genuine.

The Provider did not submit a copy or screenshot of the text that was sent to the Complainant. However, in its response to questions from this Office, it provided an example of the type of text that was sent, and it says that this includes informing the recipient of the amount of the transaction.

The Provider submits that it received a text response from the Complainant's phone at 00:52, confirming that the transaction was genuine. As a result of this, the security flag was removed. The attempted transaction at 00:51:23 had been declined as the temporary block had been in place at that time.

The Provider submits that it is satisfied that it had received two forms of security verification for the transactions: (i) the PIN authentication, and (ii) the text authentication. The Provider relies on transaction reports to note that all of the transactions attempted in the bar were made using chip and pin authentication. The Provider submits that it is satisfied that it flagged transactions in real time, and took steps to ascertain the nature of the transactions.

When asked by this Office how the Complainant's contract complied with Regulation 76(e) of the ***European Union (Payment Services) Regulations 2018*** (***S.I. No. 6/2018)*** the Provider stated that Clause 3 of the debit card terms and conditions, set out the safeguard steps and corrective measures to be taken to keep a payment instrument safe. Clause 6 sets out the procedure for notification of the customer where fraud is suspected, and the liability of the customer in situations of unauthorised transactions. Clauses 6 and 9 relate to the situations in which a card can be blocked.

In relation to compliance with Regulation 88, the Provider submits that consent for transactions was covered by Clause 5.2, and Clause 14.1 of the contract.

The Provider submits that the Complainant failed through gross negligence to fulfil his obligations under Regulation 93. In providing evidence for this submission, the Provider relies on the contents of the phone calls of **15 January 2020** between the Provider and the Complainant.

/Cont'd…

The Provider states that the Complainant admitted to remaining in possession of his card for the entirety of the night, and acknowledged that he did receive the authorisation text but had thought that it was for the purchase of drinks. The Complainant gave an account to four agents of the Provider to the effect that the bar staff were putting incorrect prices on the card terminal, and then getting the Complainant to enter and re-enter his pin. The Provider contrasts this account with the version given by his father, in which the latter noted that the Complainant had no recollection of the night.

The Provider submits that the Complainant's account during the initial phone call, should be given greater weight as it was given on the same day as the event, and as a first-hand experience. It notes that the account was "*cogent and coherent, and remained consistent*".

The Provider submits that the Complainant breached the debit card contract, and acted negligently, by failing to take care that the card transaction amount was correct before putting the PIN into the terminal.

In relation to the ATM withdrawals, the Provider relies on a phone call of **15 January 2020,** between the Provider and the Complainant, in which it submits that the Complainant admitted recognising those transactions.

In response to the Complainant's submission that the Provider's fraud monitoring system was inadequate, the Provider noted:

> *"The Provider, being satisfied that it was the Complainant using the card, did not deem it appropriate to put a block on all subsequent transactions, noting the acknowledgment.*
>
> *The Provider is satisfied that the security alert and temporary block immediately went into operation at the time of the attempted transaction, thus stopping the transaction, the block was not lifted until a positive response was received from the Complainant's registered mobile telephone number. The Provider is satisfied that the immediacy of the block is evidence of it being an adequate service, in that it will prevent the use of the card until further pro-active steps are taken by the user through an identified means…*
>
> *In the Provider's view, this is the most reasonable and efficient manner of handling unusual activity on a customer's card."*

The Complaint for Adjudication

The complaint is that the Provider wrongfully failed to reimburse the amounts of the transactions on the Complainant's account on 15 January 2020, which he says were unauthorised. The Complainant says in that regard that the Provider's fraud monitoring system and text alert service failed and is insufficient/inadequate.

/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 **26 October 2021**, outlining the preliminary determination of this office in relation to the complaint. The parties were advised on that date, that certain limited submissions could then be made within a period of 15 working days, and in the absence of such submissions from either or both of the parties, within that period, a Legally Binding Decision would be issued to the parties, on the same terms as the Preliminary Decision, in order to conclude the matter. Following the consideration of additional submissions from the parties, the final determination of this office is set out below.

I note the relevant transaction history for the Complainant's debit card on **15 January 2020** as follows:

Time	Merchant	Amount	Outcome
00:50:35	Bar	€692.05	Denied – Security Alert on Card
00:51:23	Bar	€203.10	Denied – Security Alert on Card
00:58:24	Bar	€691.57	Successful
01:18:05	Bar	€2,495.90	Denied – Insufficient Funds
01:20:32	Bar	€1,652.84	Denied – Insufficient Funds
01:23:11	Bar	€3.57	Successful
01:41:10	Bar	€1,042.83	Successful
01:48:35	Bar	€539.72	Denied – Insufficient Funds
01:49:23	ATM	€405.92	Denied – Insufficient Funds
01:50:16	ATM	€272.12	Successful
01:57:47	ATM	€165.09	Denied – Incorrect PIN or PIN missing
01:58:22	ATM	€165.09	Denied – Incorrect PIN or PIN missing
01:58:37	ATM	€165.09	Denied – Insufficient Funds
01:59:36	ATM	€165.09	Denied – Incorrect PIN or PIN missing
01:59:54	ATM	€165.09	Denied – Incorrect PIN or PIN missing
02:00:09	ATM	€165.09	Denied – Insufficient Funds

/Cont'd…

02:01:33	ATM	€17.91	Successful

Evidence

Some of the content of the phone call between the Complainant and the Provider on **15 January 2020** (007) is as follows:

"Complainant:	*I was in this bar here last night and we bought the first round with cash but then we started using our card after, and the bar man was-*
	…
Provider:	*I can see there just on the system that there was actually a text message sent to yourself at about 10 to one Irish time-*
Complainant:	*Yeah*
Provider:	*-Regarding a transaction for 692.05, ahm, so the response from the message was yes that was a genuine transaction.*
Complainant:	*Yeah. Because what happened was I did- he kept saying that the card wasn't working and it wasn't- my pin was being incorrect, but every time he was doing that he was taking the machine back and putting in another price and getting the pin again. That's- he was scamming me, basically. So, I assumed that it was just paying for a round of drinks but actually it was paying like 600 or paying a grand or paying etc.*
Provider:	*Yeah, so it was all the ones there in [bar] is that correct?*
Complainant:	*Yeah, that's it*
Provider:	*OK. And then it has- there's a cash withdrawal then at 10 to two, was that yourself? 272-*
Complainant:	*Eh, an ATM, yeah that was me*
Provider:	*OK so it's the ones in the bar*
Complainant:	*It's the bar one yeah, would be the-*
	…
Provider:	*I'll put a detailed note on the account anyway explaining what has happened there in regarding the different transactions and with the response then from yourself in the text message.*
Complainant:	*Yeah, OK*
Provider:	*I'll have to make them aware that there was a response to a text message, ahm, and I'll just say that you thought it was for the initial round of drinks-*
Complainant:	*Yeah*

/Cont'd…

Provider: Yeah, yeah, no, I'll note that there on the account for you"

The Debit Card Terms and Conditions, being the contractual arrangement between the parties, states:

"3.0 Protecting your Card, PIN and other Security Credentials

3.1 You should sign your Card as soon as you receive it.

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.

3.3 When making online transactions you may be required to enter a 3D Secure Passcode…

3.4 You should always protect your Card and take the greatest possible care to ensure that 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…

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

…

4.2 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 Retailor using your Card

…

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.*

ii.

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

/Cont'd…

someone else. You must inform us by calling us free of charge via the Freephone number listed on our website [www.[Provider].com](http://www.[Provider].com).

We may ask you to confirm this notification in writing within seven days (or 21 if you are abroad). You must not use the Card again.

6.2 *You can limit your own losses if you tell us immediately when your Card has been lost, stolen or used without your permission. The same applies if you believe someone else knows your PIN, 3D Secure Passcode or other Security Credentials.*

6.3 *If you use your Card as a Consumer, you are liable only for €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 if they were made:*

(a) because of any fraud or gross negligence by you.

(b) the Card was lost or stolen and the PIN, 3D Secure Passcode or other Security Credentials became available to the finder or thief or someone else had access to the Card.

(c) someone possesses the Card with your consent and uses it or gives it to someone else; or

(d) you do not co-operate fully with us or others in any investigation concerning the theft or loss of the Card or any attempt to retrieve it.

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

9.0 Ending this Agreement and Interruption to Services

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

i. *You die*
ii. *You are declared bankrupt or insolvent (under Irish or other law);*
iii. *You seek legal protection from your creditors…*
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*

/Cont'd…

vi. *We are required to do so by law, regulation or direction from an authority we have a duty to obey*
vii. *You have breached these terms and conditions or the Account terms and conditions; or*
viii. *Your account is overdrawn with an unauthorised overdraft…*
ix. *We have good reason to believe you do not wish to use your Card in the future…*

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."

I note that the card service made available by the Provider to the Complainant, is also governed by the ***European Union (Payment Services) Regulations 2018,*** the relevant provisions of which are as follows:

"Information

76. A payment service provider shall provide the following information to a payment service user:
…

(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…

…

Obligations of the payment service user in relation to payment instruments and personalised security credentials

93. (1) A payment service user entitled to use a payment instrument shall—

(a) ***use the payment instrument in accordance with the terms governing the issue and use of the payment instrument****, which must be objective, non-discriminatory and proportionate, and*

(b) notify the payment service provider concerned, or an entity specified by the latter for that purpose, without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.

(2) For the purposes of paragraph (1)(a), the payment service user concerned shall, in particular, as soon as it is in receipt of a payment instrument, ***take all reasonable steps to keep its personalised security credentials safe****.*

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.

(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.***

Payment service provider's liability for unauthorised payment transactions

/Cont'd…

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.

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.*

(4) Where a payer's payment service provider does not require strong customer authentication, the payer shall not bear any financial losses relating to an unauthorised payment transaction unless the payer has acted fraudulently.

(5) Where a payee or the payment service provider of the payee fails to accept strong customer authentication, it shall refund the financial damage relating to an unauthorised payment transaction caused to the payer's payment service provider.

/Cont'd…

(6) A payer shall not bear any financial consequences resulting from use of a lost, stolen or misappropriated payment instrument after notification in accordance with Regulation 93(1)(b), except where the payer has acted fraudulently.

(7) Where a payment service provider does not provide appropriate means for the notification at all times of a lost, stolen or misappropriated payment instrument, as required under Regulation 94(1)(c), the payer shall not be liable for the financial consequences resulting from the use of that payment instrument, except where the payer has acted fraudulently.

Authentication

120. (1) A payment service provider shall apply strong customer authentication where a payer— (a) accesses its payment account online, (b) initiates an electronic payment transaction, or (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.
…

(3) Where paragraph (1) applies, ***a payment service provider shall have in place adequate security measures*** *to protect the* ***confidentiality and integrity of the personalised security credentials*** *of the payment service user concerned."*

[Emphasis added]

Analysis

I am conscious that under Regulation 96, the Provider has the burden of showing that the disputed transactions were authorised and not affected by a deficiency in the service provided. To meet this burden, or to show gross negligence on the part of the Complainant, the Provider must provide evidence that goes beyond the mere record of the payment.

As per Regulation 97, the Provider is obligated to refund unauthorised payments made on the customer's account. However, pursuant to Regulation 98(3)(b), the customer will be fully liable for the payments in the event of a failure to comply with Regulation 93. The Provider submits that in this instance, the Complainant did not comply with Regulation 93, owing to his gross negligence.

Therefore, the first issue to be determined is whether the Complainant's conduct amounts to gross negligence.

Gross negligence is not defined in the 2018 Regulations. In its Parent Directive, ***Directive (EU) 2015/2366***, the following is stated at Recital 72:

"(72) 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***

/Cont'd…

> ***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. 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 to be null and void. Moreover, in specific situations and in particular where the payment instrument is not present at the point of sale, such as in the case of online payments, it is appropriate that the payment service provider be required to provide evidence of alleged negligence since the payer's means to do so are very limited in such cases."*
>
> [Emphasis added]

The definition of gross negligence was considered at the national level by the Supreme Court in *ICDL GCC Foundation FZ-LLC and Others v European Computer Driving Licence Foundation Ltd* [2012] 3 IR 327. In the majority judgment at 348, the Court stated:

> *"The trial judge emphasised the fact that the term was here being used in a commercial contract. It followed, in his view, that whether it was a term of art used in any particular area of law might not be particularly significant. The words had to be construed by reference to their text but in their context.* ***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.*** *Business efficacy had to be given to the clause. Thus, in order for the exclusion clause to be ineffective, it was necessary to find that any breach of contract established resulted from a* ***significant degree of carelessness*** *by the defendant."*
>
> [Emphasis added]

In determining whether the Complainant engaged in a significant degree of carelessness, I have had regard to the Provider's reliance of the Complainant's original account of the night in question. I have also had regard to the Complainant's clarification of his account, and his explanation of his memory issues.

The Complainant submits that he was not acting negligently, as he had been involuntarily drugged at the time. He has said in that respect that he was "*involuntarily incapacitated*". I am sympathetic to the Complainant's circumstances on the night in question. However, I accept that in his original account to the Provider, he confirmed his recollection that the bar staff were putting incorrect figures into the card terminal and repeatedly asking him to enter his PIN. This evidence was not rebutted by the Complainant in his submissions. Consequently, I accept the Provider's contention that this repeated re-entry of his PIN in such circumstances, amounted to gross negligence, and the Provider can rely on Regulation 98(3)(b) in this regard.

/Cont'd…

I note that thereafter, the Complainant's version of events changed and he subsequently suggested that he had little or no memory of the evening, but this does not accord with the recollection that he offered to the Provider within hours of the transactions being processed to his account. Whilst the Complainant has recently said that he has yet to rationalise what actually happened, and he says that the reality is that he can only "*fill in the gaps*", I believe that the information which he gave to the Provider in the immediate aftermath of the events of the night in question, is of relevance.

The Complainant has suggested that the Provider's fraud monitoring system is not adequate. I note that the security measures in place on the night in question were (i) the requirement of the correct PIN entered in the terminal and (ii) the temporary hold on the card, pending a response to a text message seeking verification of the transaction.

I consider that the Provider acted appropriately in placing a security alert on the Complainant's card when the transaction of €692.05 (six hundred and ninety-two Euro and five Cent) was attempted. The Complainant has referred to his history of transactions over the previous 5 years, and indeed this may have played some part in the transaction having been blocked by the Provider, pending confirmation from the Complainant. The Provider explains that once this transaction was verified via text from the Complainant's mobile phone, it did not "*deem it appropriate*" to block subsequent transactions.

I have had regard to the Complainant's submission that he surmises that he must not have had possession of his card and phone for parts of the night in question. However, I consider that a text message is an acceptable form of identity verification to the Provider. This method of communication is outlined in the Complainant's contract and indeed, once that verification had been given, the Provider was contractually obliged to facilitate the Complainant's subsequent transactions.

The first successful transaction was for €691.57 (six hundred and ninety-one Euro and fifty-seven Cent) at 00:58:24, six minutes following the lifting of the hold. As the figure was close to the verified transaction, and similar in time, I do not believe that this transaction should have alerted the Provider's fraud monitoring system.

The next attempted transaction was 20 minutes later, and for the figure of €2,495.90 significantly larger than the figure authorised by the text from the Complainant's phone. A pattern of behaviour can then be seen in the transaction history, whereby the user of the card methodically estimated the funds in the Complainant's account by attempting smaller and smaller transactions, until an attempt was successful. Six of the 17 attempted transactions were declined, due to insufficient funds and the Complainant confirmed during his phone call to the Provider that the later ATM transaction for €17.91, had been carried out by him.

I take the view that the measures which the Provider had in place to protect the security credentials of the Complainant's account were adequate, insofar as the Complainant was firstly required to verify his transaction by entering a correct PIN into the debit card terminal.

/Cont'd…

Once that PIN was entered, the Provider, recognising that the transaction was coming from abroad and noting a relatively large amount, took the precaution of blocking the transaction until such time as it could receive appropriate verification from the Complainant that the transaction was in fact authorised, and it only then released the block on the Complainant's debit card.

The Complainant has regrettably found himself in a difficult situation, as a result of the transactions debited to his account, but whilst it seems that there may have been a fraud perpetrated on him, while he was abroad, I am satisfied for the reasons explained above, that the Provider was entitled to form the opinion that the transactions arose from the Complainant's gross negligence during the night in question, and I therefore accept that there is no obligation on the Provider to reimburse those monies to the Complainant's account.

In those circumstances, on the basis of the evidence made available in this matter, I am satisfied that the Provider was not guilty of any wrongdoing and that there is no reasonable basis upon which the 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 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 December 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.