



<u>Decision Ref:</u>	2020-0125
<u>Sector:</u>	Banking
<u>Product / Service:</u>	Debit Card
<u>Conduct(s) complained of:</u>	Failure to process instructions Complaint handling (Consumer Protection Code) Dissatisfaction with customer service
<u>Outcome:</u>	Rejected

LEGALLY BINDING DECISION
OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

This complaint arises out of a current account held with the Provider with an associated debit card and security blocks placed on the Complainant's card when he attempted to carry out a number of transactions. In addition the complaint relates to poor customer service and complaint handling. The complaint also concerns an attempted fraud that was carried out on the Complainant's account in February 2019 and the allegation that the Provider did not alert the Complainant promptly enough. The Complainant also complained that on 25 November 2018, he requested for a complaint to be logged. He complains that this instruction was never carried out by the Provider.

The Complainant's Case

The Complainant holds a Visa debit card the Provider. The Complainant alleges that from 28 December 2017 and up to the end of February 2018, he had been experiencing serious difficulty using his Visa debit card as the Provider was declining to process purchases on a regular basis. The Complainant explains that these purchases ranged from online purchases to chip and pin payments and bill payments. The Complainant states that having received text messages or email correspondence from the Provider's security team and following up with the confirmation of the attempted purchase, this did not result in the transaction being processed. In addition, the Complainant states that these instances have resulted in him having to repeat purchase transactions and/or ring the Provider in order to have the transaction processed. The Complainant states that the Provider has not taken the issue seriously and failed to address the issues at the time of and following each event.

In addition, the Complainant complains that the Provider failed to investigate and resolve the issue adequately or at all and failed to follow up or appropriately address his complaint in this regard.

In addition, the Complainant noticed fraudulent activity on his account on 5 February 2019. He states that on foot of noticing this himself, he rang the Provider to alert it of the activity. He complains that he did not receive a security alert regarding the fraudulent activity prior to him contacting the Provider and that he only received this alert during the phone call.

The complaint is that the Provider failed to exercise reasonable care and skill in its dealings with the Complainant and in particular has wrongfully, unreasonably failed to facilitate him in making his transactions when he wanted to. In addition, the complaint is that the Provider fails to adequately investigate and resolve the issue and his complaint in this regard. Furthermore, the complaint is that the Provider did not alert the Complainant with sufficient promptness in relation to the fraudulent activity on his account in February 2019.

The Provider's Case

The Provider states that it temporarily blocked the Complainant's Visa debit card on a number of occasions as the card was flagged to the Provider's security systems due to an alert which triggered. The Provider submits that all transactions which flagged with monitoring systems on the Complainant's card met a particularly high fraudulent alert level. The Provider states that all security flags which were alerted to its system were done in good faith and a temporary block was placed to protect the Complainant's account in line with the Provider's security processes. The Provider does acknowledge and concedes shortcoming in the service the Complainant received on foot of the number of telephone calls he made and the conflicting information he was provided with. In addition, the Provider has accepted that there was a lapse in service in respect of the delay in responding to his complaint lodged on 25 November 2018. The Provider has offered a sum of €2,000 in recognition of the inconvenience suffered by the Complainant in relation to the events prior to 25 November 2018 and has offered a further sum of €500 in recognition of the lapse of service in failing to adequately deal with the complaint logged on 25 November 2018.

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.

/Cont'd...

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 7 February 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, I set out below my final determination.

I have carefully examined and considered the documentation furnished to me by both parties. In addition, I have had the opportunity to consider the audio of the phone calls between the Complainant and the Provider which were provided in evidence.

The Provider, in its response to this Office, listed all of the transactions affected by a security block. In total, between 29 December 2017 and 15 March 2018 there are 24 transactions affected. All but two transactions were attempted in Ireland. Of the 22 Irish transactions, 50% of these were attempted transactions with *www.lottery.ie*. 6 affected transactions occurred on the same day on 10 February 2018 and in total, 16 of the 22 attempted transactions in Ireland occurred in the month of February 2018.

The Provider has set out a detailed timeline of the events in relation to each of the affected transactions. Having considered the audio recordings of the telephone calls, I am satisfied that the Provider's narrative or description of each listed event in its response to this office accurately reflects the contents of those phone calls. It is apparent from these phone calls and the description of each of the affected transactions that the Complainant became increasingly frustrated with the regular security blocks being placed on his transactions, notwithstanding the fact that they were temporary blocks. On each occasion, the Complainant was obliged to contact the Provider in order to have the security block lifted. It was explained to the Complainant by the Provider on most occasions why the temporary security block was happening but on one occasion, the Provider stated during telephone calls that it had not placed any security block on the Complainant's card and that the declining of the card was not due to any security issue. The Provider now accepts that this was incorrect.

On another occasion, on 10 February 2018, the Provider suggested to the Complainant that a new card issue to him. The Complainant did not accept this at the time. On 14 February 2018, a team leader from the Provider's security team contacted the Complainant and it was suggested to him that he replace the card.

/Cont'd...

The Provider's team leader expressly told the Complainant that the Provider's technical team believes the issue was with the card itself. The Complainant did not accept this at the time. In the Provider's response to this office, it submits that the Provider suggested replacing the debit card but this was not suggested because there was a "problem" with the debit card. This is contrary to what the Provider's team leader told the Complainant that is, that the technical team believe there might have been an issue with the card itself.

I am satisfied, and I believe it is self evident from an objective viewpoint, that the number of affected transactions in such a short period of time is not typical and is over and above the normal amount of affected transactions that a cardholder might or should expect to experience in this short period of time.

That being said, this does not of itself mean that the Provider is guilty of any wrongdoing. As the Provider explains, and I accept, that the Provider's main concern is to protect its consumers from potential fraudulent activity and the flagging of certain transactions will automatically occur regardless of there being a possible issue with the card for the transaction. The Provider is unable to exempt a particular card or account from its security checks and I accept that there are certain transactions that might match the criteria of a specifically high fraud alert or risk to the Provider system notwithstanding the fact that it is a genuine transaction with a legitimate company. In addition, the Provider explains, and I accept that it occurred in respect of the affected transactions, that a text message or email is sent to the account holder who can then confirm that the transaction is genuine and the temporary block is removed.

Providers may, in the event of a suspicion of any fraud or unauthorised activity, block an account and advise the account holder of the block and how it may be removed. I do not believe that this permits or allows for an ongoing, continuous or regular policy of blocking transactions. This policy is clearly designed to be activated "in the event" that the Provider has a suspicion or has detected fraud or unauthorised activity on a customer's account.

The Consumer Protection Code 2012 provides as follows:

GENERAL REQUIREMENTS

- 3.1 *A **regulated entity** must ensure that all instructions from or on behalf of a **consumer** are processed properly and promptly.*

The above wording from the Consumer Protection Code 2012, obliges a Provider to ensure that all instructions from customers, which must include transactions, are processed not only *promptly* but also *properly*. Properly has to include an obligation to ensure that the instructions are being carried out legitimately, lawfully and with the authorisation of the account holder. Therefore, there is clearly a balance to be struck between the Providers obligation to ensure that there is no fraud or unauthorised activity carried out on a customer's account and the Providers obligation to ensure that customers enjoy the prompt and efficient execution of their instructions by the Provider.

The General Principles of the Consumer Protection Code 2012 provide, among other things, as follows:

GENERAL PRINCIPLES

A regulated entity must ensure that in all its dealings with customers and within the context of its authorisation it:

2.11 without prejudice to the pursuit of its legitimate commercial aims, does not, through its policies, procedures, or working practices, prevent access to basic financial services; and

In this complaint, we are dealing with 24 incidents of transactions being flagged to the Provider as being suspicious of a potential fraud or unauthorised activity. All of these incidents occurred within a short period of time. There is no suggestion by the Provider that transactions over a certain monetary threshold were being flagged.

The Provider explains that all of these affected transactions were identified in order to protect the Complainant from being the subject or the victim of fraudulent activity. In the circumstances of this complaint, while I acknowledge and accept the Provider's responsibilities and obligations, I am not satisfied that the Provider's overall policy was being implemented properly. The amount of times that the Complainant's transactions had a temporary block p on them was excessive from any objective viewpoint and it clearly caused the Complainant a significant amount of inconvenience and embarrassment.

I am also satisfied that the manner in which the Provider dealt with the Complainant was completely inadequate. Firstly, there was the suggestion that there was a problem with his card which, by the Provider's own admission, turned out to be misguided. In addition, on 10 February 2018, during a phone call, the Provider accepted that what was occurring was not acceptable and that a complaint was going to be lodged on behalf of the Complainant. On 14 February 2018, the Provider's team leader called the Complainant and promised to follow up with him following a call. The Provider acknowledges that this individual did not contact the Complainant further while his complaint was being investigated and the Provider has apologised for this. Subsequently, the Provider has acknowledged its failure to properly deal with the complaint of 25 November 2018. I accept that the Complainant received poor customer service and that his complaint was not dealt with properly.

In relation to the complaint regarding the failure to receive any text message alert in respect of attempted fraudulent activity in the Complainant's account on 5 February 2019. The Complainant states that he contacted the Provider having noticed the activity online and that the text message alert was received subsequently. I'm not satisfied that this is consistent with the contents of the call of 5 February 2019 from the Complainant to the Provider. In this call, the Complainant confirms that he got a text message from Visa about a number of transactions and on foot of this he checked his account online.

/Cont'd...

Having considered all of the foregoing, I am satisfied that the overall offer of compensation to the Complainant of €2,500 in respect of the totality of the complaint is reasonable and is an adequate level of compensation. Accordingly, I do not uphold this complaint.

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.

**GER DEERING
FINANCIAL SERVICES AND PENSIONS OMBUDSMAN**

6 March 2020

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.**