



<b><u>Decision Ref:</u></b>	2019-0301
<b><u>Sector:</u></b>	Banking
<b><u>Product / Service:</u></b>	Debit Card
<b><u>Conduct(s) complained of:</u></b>	Dissatisfaction with customer service Delayed or inadequate communication
<b><u>Outcome:</u></b>	Partially upheld

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

**Background**

This complaint relates to a security block placed on the Complainant's card by the Provider against which this complaint is made, when she attempted to pay a credit card issued by a third party bank through An Post.

**The Complainant's Case**

The Complainant holds a credit card account with another Bank. She states that she pays this in full each month through the Post Office with her debit card held with the Bank which is the subject of this complaint. The Complainant states she received a text message from the Bank asking her to confirm that it was her making the payment. She was told by the Bank that this was a fraud prevention measure. She states that she accepted this explanation on the first occasion but that she no longer does. The Complainant states that she called to the Post Office again to attempt the payment and her debit card payment was declined a second time. The Complainant states that having made enquiries with the Bank, the Bank informed her that her confirmation text was only valid for 24 hours and as 48 hours had elapsed it was declined again for security reasons.

The Complainant states that the Post Office staff had told the Complainant/the reason for her card being declined might be that there were no funds in her account. The Complainant

states that this was an embarrassment for her in front of other people waiting behind her. The Complainant states that this was untrue and that there was money in her account.

The Complainant explains that she has paid her monthly credit card account through the Post Office for years since her Bank had ceased this method of payment a number of years ago.

The Complainant states that she was told that if she telephones the security department each month, 24 hours prior to payment, they could guarantee payment, otherwise it would be declined again.

The Complainant states that this is unsatisfactory and unreasonable. She does not wish to set up online banking as has been suggested as an alternative. The Complainant wants the Bank to allow her to have control over payment transfers at the Post Office and that when the Bank communicates by text and she responds "yes", a transfer should be permitted without having to make contact with the Bank.

The complaint is that the Bank failed to exercise reasonable care and skill in its dealings and communications with the Complainant and in particular has wrongfully, unreasonably failed to facilitate her to pay her credit card as outlined above and failed to communicate adequately with her.

### **The Bank's Case**

The Bank states that it temporarily blocked the Complainant's Visa debit card as the card was flagged to the Bank's security systems due to an alert which triggered. The Bank explains that at the time, it was experiencing an increase in fraudulent activity in customers' accounts, particularly for transactions being made through An Post. As a security measure, the Bank explains that it put extra precautions in place for all large transactions being attempted through An Post. The Bank states that these extra security measures were in place to protect its customers from potential fraudulent activity.

### **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 29 August 2019, 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 in evidence to me by both parties. The Bank provided the details of the security text messages sent to the Complainant on **29 January 2018 and 31 January 2018** respectively. In relation to the text message and on **29 January 2018**, the Bank was able to show that it issued to the Complainant's phone at 13:29 and that the Complainant responded by text message at 16:37. The response by the Complainant confirmed that she recognised the transaction. The Bank removed the temporary security block at 16:49, some 12 minutes following receipt of the Complainant's affirmative response. The Bank sent a further text message, a copy of which has been furnished to this office stating, "If you responded 'yes' no further action is required by you at this time".

I have also carefully examined the chronology of events which led to the complaint. The Complainant's transaction was declined at An Post on **29<sup>th</sup> January 2018** when she attempted to pay €913.41 from her Visa Card using a debit card issued by the Bank. The Bank sent a text message at 13:29 asking, "Do you recognize this transaction? We will restrict the use of your card until we hear from you." I note that this is an automatic block placed on the card due to the nature of the transaction and the suspicion of fraud as described above. At that time, there was no way for the Complainant not to have her card declined due to the nature of the security measures.

The Complainant replied, "Yes" to the text which was received by the Bank at 16:37 and the card was unblocked at 16:49. However, the Complainant was not informed that the type of transaction she had wanted to make was now only possible for a period of 24 hours, starting from the time the block on the card was removed. Although she was not made aware of it, this meant the payment could only be made until 16:49 on **30 January**, if it was attempted again after this time, it would again be blocked. Unfortunately, this is what happened.

On **31 January**, the Complainant tried to make the same transaction only to have her card declined at An Post a second time. On this occasion the Bank sent the same text message at

/Cont'd...

15:39 and she replied, "Yes" at 15:43. She then attended her local branch of her Bank where a member of staff [BH] telephoned the security team to enquire on her behalf for the reason why the card had been declined.

The security team member acknowledged the previous block and said that the current block had been removed therefore, if she processed the transaction in the next 24 hours it would go through.

The communication on this occasion was clearer than what happened on 29 January when the Complainant was not informed of the temporary nature of the availability of the card for the transaction she wished to make.

I believe the Bank did not communicate effectively to the Complainant the temporary nature of the availability of her debit card to make the transactions she sought to complete. The fact that she was not told of the existence of the 24 hour window of opportunity nor when the 24 hours started, caused the Complainant inconvenience and embarrassment, since she attempted the same transaction and was told again, in public, that her card had been declined. The Complainant has stated that this was also very embarrassing for her.

I note the security concerns of the Bank and accept that in this regard it has acted in good faith to ensure the security of the Complainant's account. Nevertheless, very important information was not made clear to the Complainant.

Audio recordings of the two telephone calls have been provided and I have considered the content of those calls. The first call was from Complainant's branch to the Bank on **31 January 2018** enquiring as to why a block was put in place. It was clear the Complainant was in her branch at the time in the presence of the caller. The Bank stated that on **29 January 2018** the Complainant's transaction was flagged and the hold was taken off but that the lifting of the hold only lasts for 24 hours and that it was flagged again on **31 January 2018**. The Bank explained that it was experiencing so much fraud through Post Offices which is why they were 'flagging' those transactions.

In the second call on **2 February 2018** from Complainant to the Bank's Debit Card security telephone number, the Complainant explained she wished to make a complaint about her transactions being declined twice in a 48 hour period. The Bank explained that they were experiencing a large volume of fraudulent transactions in recent periods. It was explained, amongst other things, that there was extra protection put in place for Post Office transactions of a particular size.

The Bank has provided a copy of the terms and conditions applicable to the Visa debit card. The Bank relies on clause 11.9 which states:

*In the event we suspect or detect any fraud or unauthorised activity on your account, we will advise you via phone call, SMS message or email as appropriate. If we deem it necessary we may block your account and will advise you of the block and how it may be removed.*

/Cont'd...

The complaint is that the restriction placed on her ability to make the payments as she wishes is totally unacceptable and is an unreasonable inconvenience for the Complainant.

The Complainant states that the only other options given to her were online transactions which she states is not an option for her or to make a telephone call to the Bank in advance of making the transaction, which also is an unreasonable inconvenience. The Bank on the other hand, states that while it does not underestimate the inconvenience that may have been caused to the Complainant during the blocking of her card, it states that its action were solely based on protecting the Complainant's account at a time that fraudulent activity had increased in transactions completed in the Post Office. The Bank says that it has provided the Complainant with alternative payment options as well as suggesting that the Complainant make the Bank aware if she was going to make large payments using her Visa debit card through An Post in the future.

The terms and conditions applicable clearly permit the Bank in the event of a suspicion of any fraud or unauthorised activity to block an account and to advise the account holder of the block and how it may be removed. From my reading of this provision, it clearly does not provide for an ongoing, continuous or perpetual policy of blocking transactions.

This policy is clearly designed to be activated "in the event" that the Bank has a suspicion or has detected fraud or unauthorised activity on a customer's account.

In addition, 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 Bank to ensure that all instructions from customers, which includes 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 Bank's obligation to ensure that there is no fraud or unauthorised activity carried out on a customer's account and the Bank's obligation to ensure that customers enjoy the prompt and efficient execution of their instructions by the Bank.

This complaint relates to two incidents of transactions being flagged to the Bank as being suspicious of a potential fraud or unauthorised activity. The Bank has explained that the reason for this is that around this particular time the Bank had become aware of a significant and increased volume of fraudulent transactions being carried out through An Post. Accordingly, transactions over a certain threshold by a certain age cohort were being flagged and the procedure as prescribed by clause 11.9 of the terms and conditions applicable to the Visa debit card were being invoked.

I have also examined this complaint in the context of the Payment Services Directive. Part

/Cont'd...

Five, Chapter 2, "Authorisation of Payment Transactions" states as follows:

Paragraph 69, 'Limits of the use of payment instruments'.

- 69.2 *If agreed in the relevant framework contract, a payment service Bank may reserve the right to block a payment instrument for objectively justified reasons related to the security of the payment instrument, any suspicion of unauthorized or fraudulent use of the payment instrument or, in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil his or her obligation to pay.*
- 69.3 *In such cases the payment service Bank shall inform the payer in an agreed manner of the blocking of the payment instrument and the reasons for it, if possible before the payment is blocked and at the latest immediately after the blocking, unless giving such information would compromise the security of the payment service Bank or is prohibited by another law.*
- 69.4 *The payment service Bank shall unblock the payment instrument or replace it with a new payment instrument once the reasons for blocking no longer exist.*

In this particular complaint, the Bank has submitted a copy of the terms and conditions and has complied with them. The Bank has specifically referenced the type of fraud it sought to prevent, the demographic of the victims of the fraud they sought to counter and location at which the frauds were being perpetrated. In addition, the Bank has specified that the more sophisticated fraudsters sought to mimic legitimate transactions.

The Bank has sought to inform the Complainant in the agreed manner under the terms and conditions at paragraph 5.7, using a text 'referral' message, when the Bank suspected fraudulent activity. The Bank has also, as required by the Directive, unblocked the card promptly when the reason for the block no longer applied.

It seems clear that the Bank has acted in accordance with the Consumer protection Code in the best interests of its customer, even though its decision to maintain the requirement to pre-clear transactions through An Post causes the Complainant a degree of inconvenience.

The Bank explains that this was in order to protect its customers from being the subject or the victim of the increased fraudulent activity that was suspected of being carried out or that was being carried out through An Post. In the circumstances of this case, while I acknowledge and accept the inconvenience, annoyance and frustration of the Complainant arising out of the two incidents where her transactions were blocked, I accept that the Bank acted reasonably in weighing up its obligations and in taking the actions that it did and that it would not be reasonable to expect the Bank to make exceptions for one particular customer where an overall policy has been implemented for legitimate security reasons.

I also understand the ongoing inconvenience and frustration that this issue is going to cause the Complainant. However, I do accept the need to ensure the security of its customers'

/Cont'd...



accounts and I accept it is not possible to exempt one customer from the general security systems in place.

That said, I do believe the Bank's communication with the Complainant could have been much better. The Bank itself identified the Complainant as being of a certain demographic and at partial risk. The communication about the block of the transaction was wholly inadequate.

After the Complainant had replied, "Yes" by text that she recognised the transaction and that it was a valid transaction she received a text stating "Thank you for your reply. If you replied 'No' a [Bank] security agent will be in contact with you as soon as possible to discuss further. If you replied 'Yes' no further action is required by you at this time".

The Bank was asked the following question by this Office:

"Following her reply to the security text, be it by text or telephone did the Bank then advise the Complainant that the transaction must take place within 24 hours in order for it to be approved?"

In its response dated 25 October 2018 the Bank stated:

"Following the Complainant's response, the Bank sent a further text message (as shown below) confirming ' if you responded 'yes' no further action is required by you at this time". The Complainant visited her branch [location] on 31 January 2018 and questioned why her card was blocked by the Bank on 29 January 2018. The Complainant spoke with [named official] who contacted the Bank's Security team with the Complainant present. During this call the Security agent advised [named official] that should the Complainant process the transaction within the next 24 hours, it would go through for her as the temporary block had been removed. As the security measures were in place for An Post transactions, the Bank could not guarantee these transactions would not flag to our system again".

The Complainant states in her letter to this Office of 8 October 2018 that:

"The bank's response is not correct. They did not inform me in their text of 29 January that I had only 24 hours to make a transfer. It was not until after the second refusal when I visited [named] Branch and [named official] made contact with a bank representative over the phone that she informed me that there was a 24 hour time restriction".

The Bank responded by letter dated 25 October as follows:

"The Bank sent a text message to the Complainant requesting her to confirm if she recognised the transaction for An Post. The Complainant responded to the Bank's text confirming the transaction as genuine.

On 31 January 2018 the Complainant was in [Bank branch] where a staff member [named official] contacted the Card security team on the Complainant's behalf. During [named official] call the card security agent advised [named official] that should the Complainant make the transaction within 24 hours, it will be authorised, however after this period of

/Cont'd...

time the Bank cannot guarantee the card will not flag to its security systems again.

[Named official] relayed this information to the Complainant.

The Bank would like to note that at no stage did anyone advise the Complainant that she will have 'only' 24 hours to make the payment. The Bank submits that making the payment within 24 hours after the temporary security block is removed will ensure the security block will not affect the payment for the next 24 hours. However after 24 hours the Bank cannot guarantee that the card will not flag to our security systems again".

It is disappointing that the Bank cannot see that its communication with the Complainant was inadequate. In my view, the Bank did not communicate clearly to the Complainant what she needed to do after her card was blocked on the first occasion in order to avoid a recurrence.

While the Bank seems to be saying in its response above that it was not the case that the Complainant "only" had 24 hours to make the payment without having it blocked, this appears to actually be the situation.

This was borne out by the second blocking of her card when the reason given was that she did not carry out the transaction within 24 hours.

Indeed, it is not clear to me at this stage whether or not the Complainant "only" had 24 hours after the transaction was unblocked to attempt to make it again.

With regard to the provision of information to a consumer the Consumer Protection Codes state that a regulated entity must ensure that all information it provides to a consumer is clear and accurate, and that key items are brought to the attention of the consumer. The method of presentation must not disguise, diminish or obscure important information.

Provision 4.1 of the Consumer Protection Code 2012 states that:

4.1 A regulated entity must ensure that all information it provides to a consumer is clear, accurate, up to date, and written in plain English. Key information must be brought to the attention of the consumer. The method of presentation must not disguise, diminish or obscure important information.

I believe the Bank's communication was not clear and greatly inconvenienced the Complainant. Indeed, I believe its communication by way of response to the complaint to this Office continues to be unclear.

For this reason, I partially uphold the complaint and direct the Bank to pay a sum of €400 in compensation to the Complainant. I also direct the Bank to write to the Complainant explaining why her transactions, that are the subject of this complaint, were declined so she may present the correspondence to the Post Office should she wish.

/Cont'd...



## **Conclusion**

My Decision pursuant to **Section 60(1)** of the **Financial Services and Pensions Ombudsman Act 2017**, is that this complaint is partially upheld, on the grounds prescribed in **Section 60(2) (f) and (g)**.

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 compensatory payment to the Complainant in the sum of €400, 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 the Bank to write to the Complainant explaining why her transactions, that are the subject of this complaint, were declined so she may present the correspondence to the Post Office should she wish.

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.**

**GER DEERING  
FINANCIAL SERVICES AND PENSIONS OMBUDSMAN**

23 September 2019

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

/Cont'd...

**(b) ensures compliance with the Data Protection Regulation and the Data Protection Act 2018.**

