An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

Decision Ref:	2019-0054
Sector:	Banking
Product / Service:	Debit Card
Conduct(s) complained of:	Refusals (banking)
Outcome:	Rejected

LEGALLY BINDING DECISION
OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

Background

This complaint concerns a block placed on the Complainant's debit card as a fraud prevention measure, which resulted in a genuine transaction being initially refused.

The Complainant's Case

The Complainant holds a current account with the Provider with an associated debit card facility. He says that when he tried to purchase prize bonds on his debit card to the value of €2,000 in **April 2018**, the transaction was blocked on two occasions. He received a phone call from a private number claiming to be from the Provider seeking confirmation that he wanted to make the transaction in question. When the Complainant confirmed, the block was removed and the transaction was processed.

The Complainant wants the Provider to desist from ringing customers from a private number in relation to sensitive issues and he seeks an explanation as to why the Provider blocked the transaction in circumstances where six similar transactions were carried out by him without query, the previous year. He also seeks a change in the practice whereby he is asked to seek permission in advance for an exemption on his account in order to prevent a security hold. The Complainant also seeks compensation for what he describes as an "*embarrassing, time-wasting issue*".

The Provider's Case

The Provider states that the security hold was placed on the debit card at 09:37 and removed at 09:39 on 3 April 2018 once the Complainant spoke to a member of the Provider's financial crime prevention unit (FCPU) and the transaction was confirmed as genuine. It says that the security hold was placed on the account due to the Provider's monitoring system which seeks to alert it to potentially fraudulent transactions. It explains that alerts are driven by most probable fraud scenarios based on prevailing trends and that transaction monitoring is offered by the Provider when suspicious patterns or trends present themselves. It has argued that the use of unknown numbers in this context is for security reasons. It explains that the reason for the concern was due to the manner in which the transaction was processed – as a 'money transfer' – as problems can arise in disputing such transfers in the event that they are deemed fraudulent.

The Provider suggests that if the Complainant wishes to complete a similar transaction in the future, it would be best practice to contact the FCPU in advance, and seek an exemption to prevent a security hold being placed on the card.

The Complaint for Adjudication

The complaint is that the Provider wrongfully blocked a transaction on the Complainant's current account on 3 April 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.

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 6 February 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

/Cont'd…

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.

On 3 April 2018, the Complainant attempted to purchase prize ponds online with his debit card. He tried to use his card twice, but the payment attempts did not go through despite there being sufficient funds in the account to meet them.

Before he tried a third time, he received a telephone call from a private number, which turned out to be an agent of the Provider. The Provider's agent explained that the transaction triggered a security block on the Provider's system and so he was ringing to confirm that the transaction was genuine.

Having confirmed that the transaction was a genuine one, the Complainant used his debit card again and this time the transaction was processed.

The time that elapsed from the initial (unsuccessful) attempt to the third (successful) attempt was between 2 and 3 minutes.

A similar chain of events unfolded again on 19 April 2018.

In this instance, the block was placed by the Provider on a transaction that was not fraudulent or unauthorised. In the context of this Decision, and the jurisdiction of this office, I must decide whether or not the block was placed wrongfully, in the sense of being placed on an unreasonable or unfair basis, or outside the account terms and conditions. The Complainant also takes issue with the fact that the Provider contacted him from a hidden or private number. Finally, the Complainant also suggests that the Provider is acting wrongfully or in an unreasonable or unfair manner in suggesting that the Complainant contact it in advance, each time he wishes to make a transaction of this nature going forward.

Card Terms and Conditions

The relevant applicable terms and conditions for the Complainant's card are as follows:

> *"If we suspect that a Card and/or Account is being used improperly, fraudulently or in breach of the Agreement or of actual or suspected security threats, we may decline to authorise any further transactions on the Account. We will endeavour to contact you before we take this decision but this may not be possible. You hereby agree and authorise us to take such actions as we deem necessary including suspending the Account in such circumstances."*

/Cont'd…

The Provider therefore, has a contractual entitlement to suspend or (as occurred in this case) place a block on, a debit card pending further investigations into the nature of transactions being effected.

Of course, the mere fact the terms and conditions allow for such a course of action, does not make it reasonable or fair in all circumstances.

The Provider by way of final response explained to the Complainant that the transaction was blocked because the online transaction being attempted, is processed as a 'money transfer' and accordingly the Provider's systems automatically hold payment of such a transaction until the cardholder has confirmed that it is authentic. The Provider states that this "flagging" is a response to trends in fraudulent activity, and also because a transaction that is processed as a "money transfer" does not offer the same protection to a customer (in terms of the customer's entitlement to a refund) in the event that it is later flagged, as being unauthorised.

The Provider in its final response stated that:-

> *"Our FCPU have advised that if you are to complete a transaction such as this again, it would be best practice to contact them prior to processing, for them to apply an exemption to your Account and avoid a security hold being placed on your card".*

Upon receipt of this letter, the Complainant appears to have overlooked the reference to "*a transaction such as this*". He telephoned the Provider's fraud unit over a dozen times seeking pre approval for every transaction he intended to make thereafter. When he called the fraud unit he explained that he was in a possession of a letter that told him to contact them each time he intended to make a transaction. It was consistently clarified to him that this "pre authorisation" procedure only applied to unusual transactions such as the one to purchase prize bonds for €2,000, which formed the original basis of this complaint.

The Complainant repeatedly told the Provider he had no way of knowing what constituted an "unusual transaction", and so he was going to call the FCPU before every transaction.

These telephone calls varied from good natured exchanges to fraught ones, and indeed varied in length from a couple of minutes to forty minutes long.

Analysis

The Provider has furnished extensive submissions in response to this complaint. In essence, the Provider has a range of automated systems which identify if certain criteria on a transaction are met and, in that event, automatically trigger a block until authentication is received from the cardholder. This is a system which offers potential benefits to the Provider's cardholders, in the form of such added protections.

The Complainant points out that if someone checked his account history prior to effecting the block, that person would see that prize bonds online purchases for €1,000-€2,000 are a

/Cont'd…

regular feature on his account and so a block would not be necessary. This unfortunately does not take account of the fact that the block is an automated response to the transaction type, it is not necessarily reviewed by a staff member prior to it being applied. Given the number of transactions carried out each hour of each day around the country, and the speed with which they can be effected, it would not be reasonable to expect a Provider to retain the services of sufficient staff to manually review every transaction within a few seconds prior to authorisation. Quite simply, it would not be practical. In that regard, the Complainant's demand on the telephone for the person responsible to "*get their P45*" is misconceived, in my opinion.

The systems operated by financial service providers are updated and altered as more information about fraud trends is obtained. These systems are in place for the benefit of every customer of every provider, including the Complainant himself.

The problem in this particular instance is that the Complainant regularly makes a specific transaction that, although completely above board and authorised by him, triggers the block response from the Provider's automated anti-fraud detection measures.

The Complainant is then left in a position where, to avoid this happening, he is requested by the Provider to contact its fraud department prior to effecting a transaction of that nature.

I am not satisfied that the Provider's final response was misleading or unclear in the manner that the Complainant appears to suggest in his phone calls. An "unusual transaction", or a transaction "such as this" clearly refers to a payment online for thousands of euro, as distinct from e.g. tapping the card in a local supermarket. A four figure online payment for prize bonds may not be an unusual transaction for the Complainant, but it could reasonably be construed as relatively unusual amongst the broader customer base and amongst consumer debit card transactions in general.

It does not appear to me that the Complainant is under any real doubt about this either – my review of his telephone calls leads me to the conclusion that he was seeking to reinforce his point, rather than to clarify any genuine misunderstanding. Some calls became fraught, but I take the view that this was not due to any misconduct on the part of the Provider or its telephone agents.

The anti-fraud measures at issue in this complaint, can indeed be a minor nuisance to individuals, but their benefits are notable in any instance where they come to the aid of a cardholder who requires their protection.

I accept that it is not possible for the Provider to amend the Complainant's own account in order for the transactions to go unhindered without altering the security system as a whole. I am not satisfied that the inconvenience of the Complainant (in being asked to contact the Provider when he wants to make an online purchase of thousands of euro worth of prize bonds) is sufficient to require that the Provider compromise the integrity of its anti-fraud measures which operate to protect the accounts not only of the Complainant but also of every other customer.

/Cont'd…

Indeed, the Complainant has shown in the phone calls furnished to this office that he has no difficulty getting in contact with the Provider, when necessary.

Providers making calls to customers from an unknown number is a matter which has been a source of concern for many consumers for some time. The concerns from customers about the practice are understandable, and equally the justifications from providers illustrate the rationale, in operating in that way.

In this particular complaint the Provider has confirmed that as of the 24 April 2018 calls made from its fraud prevention unit display an identifiable telephone number, as opposed to being from an unknown or hidden number. This is a welcome development and represents a satisfactory outcome to this particular aspect of the complaint and indeed, has no doubt been welcomed by many a customer.

Summary

In this complaint, the Complainant regularly carries out a particular online payment transaction which can trigger the Provider's automated security systems and result in a temporary block being placed on the card until the transaction is verified.

This process takes approximately 2 minutes and the inconvenience this causes to the Complainant is, in my view, outweighed by the broader consideration of protecting the security of all cardholders. Consequently, I do not accept that the Provider's actions in this respect have been inappropriate or wrongful and accordingly, I do not believe that it would be appropriate or reasonable to uphold this complaint.

I note that since the Preliminary Decision issued to the parties, the Provider has confirmed that on 15 February 2019 the Complainant contacted its Financial Crime Prevention Unit to advise of his acceptance of a gesture of goodwill of €200 which had been offered to the Complainant in a letter dated 10 May 2018. This very recent development however, has no bearing on the outcome of this Legally Binding Decision.

Conclusion

For the reasons outlined above my Preliminary Decision is therefore that this complaint is rejected pursuant to ***Section 60(1)(d)*** 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
DIRECTOR OF INVESTIGATION, ADJUDICATION AND LEGAL SERVICES

22 March 2019

/Cont'd…

Pursuant to *Section 62* of the *Financial Services and Pensions Ombudsman Act 2017*, the Financial Services and Pensions Ombudsman will publish legally binding decisions in relation to complaints concerning financial service providers in such a manner that—

(a) ensures that—

(i) a complainant shall not be identified by name, address or otherwise,

(ii) a provider shall not be identified by name or address,

and

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