An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

Decision Ref:	2020-0153
Sector:	Banking
Product / Service:	Current Account
Conduct(s) complained of:	Handling of fraudulent transactions
Outcome:	Rejected

LEGALLY BINDING DECISION
OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

The Complainants hold a joint current account with the Provider. On **12 September 2016**, the First Complainant received a text message from the Provider advising her that there were insufficient funds in the joint account to meet the upcoming mortgage loan repayment. The First Complainant then checked the account and noticed a substantial number of unauthorised transactions. The First Complainant immediately contacted the Provider to advise it of the unauthorised transactions. It was confirmed that these were fraudulent transactions executed using the Second Complainant's bank card details. The Provider cancelled the Second Complainant's bank card and commenced making refunds in respect of the unauthorised transactions on **13 September 2016**.

The Complainants' Case

The Complainants refer to a letter of complaint sent to the Provider on **27 October 2016** for a description of their complaint. This letter states as follows:

> *"On the morning of the 12th of September, 2016 I received a text to my mobile number which read: '[The Provider] will be presenting a direct debit of €2,658.37 today, however there may not be enough funds in you're (sic) a/c to cover this payment. To avoid the unpaid fee of €12.70 and to ensure successful payment, you can transfer additional money FROM any other [Provider] current account via [the Provider's online banking], or alternatively lodge cash at a lodgement machine in any [Provider] branch before 4pm today …'*

I was shocked to receive this notification, as there should have been sufficient funds in our account to meet our mortgage repayments at the time of this notification. I immediately logged into my account … only to discover that our account had been hacked into by Fraudsters and they cleared out the account, completely. There was a credit balance in our account to the sum of €3,900 just before the fraud took place together with an approved overdraft of €5,000. As a result the fraudsters were able to transact on our account over a 24 hours period using my husbands (sic) Visa Debit Card … and the loss amounted to close to €9,000.

I have since discovered, that there was no trigger on our account to prevent this fraud from happening in the first place. The fraudsters were allowed to carry out a high volume of very unusual transactions on our account over a 24 hour period, which were out of character for [the Second Complainant] and I. There should have been a flag or trigger on your systems to detect such unusual activity. Why was there no 'flag' or 'marker on your systems' to identify that a fraud was taking place. What is a real concern to [the Second Complainant] and I is that our funds are not secure with [the Provider].

… It has taken us until now to get to the point that we feel the account balance is accurate, as a result of our efforts as opposed to the efforts of [the Provider]. We are now looking for a compensation proposal for its poor service, negligence, breach of contract and breach of statutory duty …"

In their complaint to this Office, the Complainants further explain that they *"… were the victims of an (sic) horrific fraud on our current account. All of our funds were depleted over a 24 hour period."* The First Complainant explains that she woke up one morning and realised that there were no funds in their joint account. The First Complainant states that she *"… was astonished to see the number of transactions which the fraudsters had carried out over a 24 hour period, yet no trigger kicked in for [the Provider] to put a stop to this.*

The Complainants explain that they have lost total confidence in the Provider and that *"… we had to go digging for information and seek explanations from [the Provider] after the event to find out what happened and to do a reconciliation on our account. In other words, we had to proactively engage with them as opposed to them reaching out to us."*

It is submitted that *"[a] flag of some sort should have appeared on the [Provider's] systems as these transactions were taking place on our account."* The Complainants states that they have copies of the transactions which comprise *"… pages and pages of transactions with unusual entries from unusual destinations."*

The Complainants found this experience upsetting and stressful, and were very angry that their account had been the subject of fraudulent transactions. The Complainants explain that *"[t]he fraudsters had cleared out our account and used up to the maximum of our overdraft limit of €5,000. The financial recovery from this was a total nightmare and it took us some time to recover from this."*

/Cont'd…

The Provider's Case

The Provider advises that it does not know how the fraud was perpetrated on the Complainants' account. The transactions were carried out as *Mail order 'Card Not Present'* transactions. In such circumstances, all that would have been required was a bank card number, expiry date and CVV number, all of which are available to merchants both online and at point of sale. The Provider submits that even if it knew where the card in question was compromised, it would not release the name to the Complainants as this could potentially damage any Garda Síochána investigation and also put the Provider at risk of being sued by the merchant for reputational damage. The Provider states that it investigates how a transaction was carried out but does not necessarily know where a card was compromised and if it does, this information is passed to An Garda Síochána.

The Provider explains that an alert was triggered on the Complainants' account on **12 September 2016** and its monitoring team was alerted to the activity taking place. The account was then placed in a queue for investigation. The Provider advises that prior to having an opportunity to investigate and contact the Complainants, the First Complainant contacted it to raise concern regarding certain transactions on the account.

The Provider states that having confirmed the transactions did not belong on the account, it expedited the investigation, blocked the card being used to make the transactions and once satisfied that a fraud had been perpetrated, began to refund the fraudulent transactions that had been posted to the account. The Provider advises that in certain instances the merchants involved in some of the transactions refunded the Complainants' account and the Provider then re-debited the account with corresponding amounts.

The Provider states that, having provided the Complainants with the information in respect of the fraudulent transactions and the refunds, one of its agents from its Fraud Department met with the First Complainant on **13 October 2016**, to go through all of the transactions to satisfy her that the account had been fully restored.

The Provider explains that in its Final Response letter dated **2 December 2016**, it stated that all of the fraudulent transactions that had posted to the account were refunded by **13 September 2016**. The Provider states that this is correct, however, there were further transactions that had not yet posted to the account until after this date and these were subsequently refunded as and when they were received. The Provider further explains that its refunds appear on the Complainants' account statements as *REDUND* followed by the merchant name. The Provider states that refunds to the Complainants' account after **13 September 2016** were completed by the merchants themselves and the Provider had no control over these refunds. The Provider advises that this continued until **12 October 2016** at which point it was satisfied that all of the fraudulent transactions on the account had been refunded.

The Provider submits that there is no record of any further unauthorised activity in relation to this instance of fraud after this date. The Provider also advises that due to the nature of the fraudulent transactions, it could only issue a refund once the transactions had been posted to the account.

/Cont'd…

For this reason, until the Provider was satisfied that all of the fraudulent transactions had presented, it could not confirm that the Complainants' account had been fully restored until **October 2016**.

The Provider submits that it acted in the best interests of the Complainants at all times. The Provider also states that it *"… would like it noted that a Credit of €8.15 was made to the account and the Bank did not re-debit this amount; in other words the Bank over refunded the account."*

The Provider rejects the Complainants' contention that it acted negligently. While it is not obliged to monitor every transaction on an account, it does operate a fraud monitoring system as an additional service to its cardholders which incorporates a Neural Scoring engine in conjunction with certain rules and strategies. The Neural Scoring is designed to highlight possible fraudulent activity which may be out of character on a customer's account. Such transactions are identified by analysing known frauds together with information received from Visa and MasterCard.

In a further submission dated **18 January 2019**, the Provider states that the transactions were debited to the Complainants' account on **11 September 2016** and that when a transaction is processed on a card it may take a few days for it to fully post to an account. The Provider advises that it has no control over the posting of a transaction because, if fully approved, it is up to the merchant to post the transaction to the account. While some transactions may have been pending on the account, these were pending authorisation from the merchants and were not pending approval by the Provider. Once the merchant has approved a transaction, the transaction will fully post to the Complainants' account. The Provider explains that until this process is complete, it is unable to refund the transaction as there may be a chance that a merchant would reverse a transaction itself.

The Provider states that the ***European Communities (Payment Services) Regulations 2009*** do not apply in this instance as the unauthorised transactions were in US dollar.

The Complaints for Adjudication

The complaint is that the Provider failed to have an appropriate system in place to detect and prevent fraudulent activity on the Complainants' account; and failed to notify and/or engage with the Complainants once the fraudulent transactions occurred and failed to investigate what had taken place on the Complainants' account.

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.

/Cont'd…

The Complainants were 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 23 March 2020, outlining my preliminary determination 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 accept that, in accordance with Part 5 of the Payment Services Regulations 2009, the unauthorised transactions that are the subject of this complaint do not fall with the Payment Services Regulations.

Terms and Conditions

Clause 10.4 of the terms and conditions of the Complainant's account states as follows:

> *"If an unauthorised payment is made from your Account, we will … refund your Account and restore it to the way it would have been if the unauthorised payment had not happened."*

Reporting the Fraud

Recordings of telephone conversations between the Complainants and the Provider have been provided in evidence. The First Complainant contacted the Provider's fraud department on **12 September 2016** to advise it of a number of suspicious transactions that had taken place on the Complainants' joint account. I now propose to set out certain parts of this conversation:

> *"…*

/Cont'd…

Complainant: *… I have been subject to a fraud on my account I got a text this morning to say that mortgages were trying to take a payment and there was not sufficient funds in the account … I logged on immediately and there is a whole list of transactions on my card that mean nothing to me or my husband. …*

…

Complainant: *… my whole account has been cleared out to the maximum of €5,000 overdrawn limit. I don't recognise any of the transactions. All the money has been cleared out on my account. €5,000 [American donut outlet], [American supermarket chain] all of these various transactions. …*

…

Agent: *The fraudsters would compromise your card. A lot of the time it would be done through a number generator. We would see that quite a lot in fraud for [the American donut outlet].*

…

Agent: *I will go down through the transactions and for the transactions which you do not recognise, I will put them in a fraud report and send them for investigation.*

…

Agent: *What will happen is once I send away the fraud report to the investigation team they will contact you within two working days on the phone number that we confirmed earlier on and then usually approximately five working days the whole investigation should be completed.*

…

Agent: *What you can do in the meantime is you can look for an overdraft to the value of the fraud …*

…

Agent: *I am going to cancel your card and I am going to reissue you with a new card.*

…

Agent: *… it looks like it was done over the internet so it looks like it was done through a number generator in which they keep selecting numbers and they would send in a small amount just as a test just to see if there are any funds in the account.*

…

Complainant: *Am I going to be hearing back from you.*

/Cont'd…

Agent: *No it will be from the investigation team.*

Complainant: *Can they prioritise it in terms of getting my account restored …*

Agent: *I can send an email on your behalf.*

…

Agent: *I am going to put you on hold and see if the transactions were made on your card or your husbands card.*

Agent: *Yes it is [the Second Complainant's] card unfortunately.*

Complainant: *You are not going to cancel my card are you?*

Agent: *No your card is fine. I have to cancel his card now and issue him with a new card. I am going to do the fraud report now and send this through along with all of the information which you sent to me.*

…

Agent: *… The investigation team will try and get the funds back from the fraudsters …*

…

Agent: *I will send the fraud report for you now. When the investigation is complete you will get a text message. You will need to ring the bank if you are looking for an overdraft. I will give you the fraud reference number …"*

Meeting with the Fraud Investigator

The First Complainant met with a representative of the Provider's Fraud Investigation Team on **13 October 2016**. The Provider has provided a statement from this individual dated **21 August 2018** which states:

> *"I was asked by my manager to meet with [the First Complainant] so that we could go through the fraudulent transactions on her account and to re-assure her that all fraudulent transactions had been refunded in full. We met in the [branch] on 13/10/2016 as this was close to where [the First Complainant] worked.*
>
> *We sat down and went through a Transaction History print out of both the fraudulent transactions and the refunds which I had highlighted in separate colours. This took over an hour to complete as we literally went through each fraudulent transaction and cross-border fee and marked off the corresponding refund with a pen.*

/Cont'd…

I apologised to [the First Complainant] for the inconvenience caused and from what I gathered she was happy at the end of the meeting that all refunds were accounted for. I also advised her that if she was still unsatisfied with the outcome that she could write a formal letter of complaint and a full investigation would be carried out."

Complaint to the Provider

The Provider confirmed receipt of the Complainants' letter of complaint dated **27 October 2016** (outlined above) by letter dated **9 November 2016** advising that it was working on resolving the matter and it would write to the Complainants by **30 November 2016** or earlier if possible. The Provider wrote to the Complainants on **30 November 2016** stating that it was not yet in a position to issue a final response but it hoped to write to the Complainants by **3 January 2017**, by which time it hoped to have completed its investigation. The Provider issued a Final Response on **2 December 2016**, stating:

"Firstly, I would like to apologise for any inconvenience this matter has caused you and I thank you for your patience while I worked to resolve it for you.

I understand your complaint relates to fraudulent activity on your Visa Debit Card on 11 September 2016. I note from your complaint you remain unhappy with regards to the investigation process and are dissatisfied that you were not contacted when these transactions debited.

I referred this matter to our Fraud Investigations Team for review and response. Our records confirm that on 12 September 2016 you contacted our Fraud Security Team on foot of a text message you received from the [Provider], confirming there was insufficient funds in your account to meet your Mortgage repayment. On this call you noted that several transactions on your account were fraudulent.

The Fraud Security representative at this time took your fraud report and assigned this to our Investigations Team. As you stated during this call that it was urgent you had [no] access to funds, the representative requested that your case be worked as a priority.

Our Fraud Investigations Team prioritised the investigation of your case and on 13 September 2016 your account was fully refunded in respect of all of the fraudulent transactions which had posted to your account. You also had a number of merchant refunds on your account which I appreciate may have caused some difficulty when attempting to reconcile your account.

In relation to your comments that the Bank should have a trigger in place to prevent fraud, the Bank is not obliged under the terms and conditions of use of the Visa Debit Card to monitor all cardholder's transactions. The Bank, however, does operate a fraud monitoring system as an additional service to its cardholders. This is designed to highlight possible fraudulent activity which may be 'out of character' on customers' accounts.

/Cont'd…

It is not possible for the Bank to monitor every transaction on each customer's account. Instead, the Bank attempts to identify out of character activity by analysing known frauds, in addition to information received from Visa and MasterCard.

In your case, your account did 'flag' to our system on 12 September 2016. When an account triggers to our systems it will queue and await review from a Security Specialist. Before the Bank had the opportunity to contact you, you contacted us to query the transactions on your account.

I note you requested to meet with our Fraud Investigations Team in [the Provider's branch] to go through each transaction and refund to ensure all fraud had been fully refunded. [The Provider's] Fraud Investigator, met with you on 13 October 2016 in [the Provider's branch] and went through all transactions with you in detail. [The Provider's Fraud Investigator] has advised that you were satisfied with the outcome of your meeting and understood all transactions were fully refunded.

I acknowledge fraudulent activity left you in a difficult position with regards to funds, however I am satisfied that your case was prioritised and refunded within two days of you reporting these transactions. Fraud cases can take up to 10 working days to be fully investigated. The Bank further assisted you by meeting with you personally to help you reconcile your accounts with you, and ensure that you were not without funds on your account …"

Analysis

The First Complainant, having become aware of the unauthorised transactions on the joint account, promptly contacted the Provider to report the activity on the account on **12 September 2016**. The Provider advises that it was also alerted by its own systems to this activity and the Complainants' account was placed in a queue for investigation by its fraud investigation team. However, before it had the opportunity to contact the Complainants, the First Complainant contacted the Provider on foot of a text message she received regarding an upcoming mortgage payment. While this is the Provider's position, the Provider has not furnished any evidence to demonstrate when the Complainants' account was flagged or placed in the queue for investigation. Furthermore, it is not clear from either the Complainants' submissions or the Provider's submissions what, if any, correspondence was sent to the Complainants or contact made with them regarding the detection/investigation by the Provider of the unauthorised transactions.

The parties have provided account statements in respect of the Complainants' joint account. From a review of these statements, I see that the first unauthorised transaction posted to the account on **13 September 2016**. This was then followed by a substantial number of very unusual transactions. The transactions were in different currencies and ranged from as low as £0.02 to $416.51. I note that roughly 7 transactions relate to Irish vendors and it is not clear whether these were in fact unauthorised.

/Cont'd…

The balance on the account before the first apparent unauthorised transaction was approximately €4,190 and the balance after the transactions posted was €1,065. The Complainants maintain the position that *"All of our funds were depleted …"* and *"… the loss amounted to close to €9,000."* However, having reviewed the account statements, the amount debited from the account appears to amount to approximately €3,125 [€4,190 minus €1,065]. I find that while there were insufficient funds in the account to meet the upcoming mortgage payment, there is no evidence to suggest that the account was overdrawn as a result of the unauthorised transactions or that the loss from the transactions amounted to almost €9,000 - contrary to the Complainants' submissions.

The account statements further demonstrate that refunds from the Provider as well as refunds from other vendors began to post to the account on **14 September 2016** with a number of re-debits also taking place. The Provider refunds appear to have completed on **14 September 2016** and the vendor refunds, together with any re-debits appear to have continued until in or around **6 October 2016**.

The First Complainant met with one of the members of the Provider's fraud investigation team on **13 October 2016** to discuss the transactions. While the high number of refunds and re-debits may have caused confusion and concern for the Complainants, I note that the Complainants have not furnished any evidence to suggest that following the refunds and re-debits, their original account balance was not restored.

The Provider states that, while it has measures in place to detect fraudulent activity, it is not obliged to monitor every transaction on an account. I note that the Complainants have not identified any contractual or legal obligation that requires the Provider to do so. In the circumstances of this complaint, I am satisfied that the Provider's contractual obligations are contained at clause 10.4 of the account's terms and conditions. Taking into consideration that the unauthorised transactions began to post to the account on **13 September 2016**, refunds promptly commenced on **14 September 2016** and the account was fully restored in or around **6 October 2016**; I accept that the Provider discharged its contractual obligations.

Therefore, I am not satisfied that simply because unauthorised transactions occurred on the Complainants' account over the course of a 24 hour period, despite the extent of these transactions, the Provider's fraud detection and prevention system was flawed or inadequate. With this in mind, the Complainants have not demonstrated how the Provider's system failed or that the Provider breached any of the obligations it owed to the Complainants.

The steps taken by the Provider in respect of the unauthorised transactions prior to the First Complainant's telephone call are not discernible from the evidence in this complaint. However, I do not accept that because the First Complainant contacted the Provider before the Provider contacted either of the Complainants establishes any wrongful conduct on the part of the Provider.

/Cont'd…

As noted above, the level of the Provider's engagement with the Complainants following the reporting of the unauthorised transactions is unclear. However, I note the Provider's representative met with the Complainants and I welcome this response by the Provider. Furthermore, I note that during the telephone conversation which took place between the First Complainant and the Provider on **12 September 2016**, the Provider's agent advised the First Complainant that *"… once I send away the fraud report to the investigation team they will contact you within two working days on the phone number that we confirmed earlier on and then usually approximately five working days the whole investigation should be completed. …"*

In light of the evidence and submissions in this complaint, I am satisfied that the Provider investigated the activity which took place on the Complainants' account. This is, in part, evident from the almost immediate refund of the unauthorised transactions.

Finally and most importantly, I note the Provider moved very quickly to identify and refund the unauthorised transactions. For this reason, 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

16 April 2020

/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.