An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

Decision Ref:	2019-0184
Sector:	Banking
Product / Service:	Current Account
Conduct(s) complained of:	Disputed transactions Failure to process instructions in a timely manner
Outcome:	Upheld

LEGALLY BINDING DECISION
OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

Background

This complaint relates to the Complainant's current account held with the Provider.

The Complainant's Case

The Complainant submits that six fraudulent transactions were carried out on his account with the Provider, totalling the sum of €12,030.84.

The Complainant states "*this whole situation is causing me severe stress, both physically and mentally and severe financial difficulty*". The Complainant submits that he had informed the Provider "*of the theft/missing bank card, driving licence and university identification, as soon as I realised that they were missing/stolen*". The Complainant submits that he never received a replacement card or PIN "*despite the fact that [the Provider was] well aware that my PIN had been compromised earlier".* The Complainant states that *"I specifically asked [the Provider] to send my 2nd replacement card and a new PIN to my local [Provider Branch] but [it] still sent the 2nd replacement card to my address and still did not send me a new PIN*". The Complainant submits that the Provider is negligent for failing to send him a new PIN for both the first and second replacement cards.

The Complainant submits that the Provider initially confirmed that it would refund the fraudulent transactions, but subsequently refused to honour its commitment. The Complainant states "*This whole situation has caused me severe depression and anxiety, due*

to lack of funds I have been having difficulty paying my house rent. This whole situation has also affected my marriage…".

The Complainant states that "*Total 12,030.84 [was] taken out fraudulently from my account. I would like to get full refund and ask for compensation due to mishandling of my case/claim*".

The Provider's Case

The Provider submits that it had refunded alleged fraudulent transactions, which occurred on the Complainant's current account on 1 March 2017 and 2 March 2017, totalling €2,216.03. It submits that these transactions occurred following Chip and PIN authorisation on the Complainant's debit card ending in '0820. The Provider submits that on 2 March 2017, during a telephone call in which the Complainant raised these transactions as being fraudulent, its agent cancelled debit card ending in '0820 and ordered a replacement debit card for the Complainant, following its process in such circumstances. The Provider submits that an investigation into the alleged fraudulent transactions ensued, which resulted in the refund of €2,216.03 being applied to the Complainant's current account on 9 March 2017.

The Provider submits that further alleged fraudulent transactions were applied to the Complainant's current account on 8 March 2017 and 9 March 2017, totalling €11,438.95. The Provider submits that these transactions occurred following Chip and PIN authorisation on the Complainant's debit card ending in '1873, which was ordered in replacement of the Complainant's debit card ending in '0820 when the original set of alleged fraudulent transactions were raised with its fraud team on 2 March 2017.

The Provider submits that it "*found fraud cases …2869, …2889 and …1973 detail 5 cash withdrawal and point of sale transactions totalling €11,438.95 that took place on 8 and 9 March 2017*". The Provider submits that its Fraud Department conducted an investigation into the Complainant's claim based on the information he provided during his fraud report call. The Provider states that "*They reached a decision to decline your claim based on their decision to close your account in line with [the Provider's] Personal and Private Banking Terms and Conditions*".

The Provider submits that it has a fraud prevention system that monitors transactions that take place on its customers' accounts for activity that is in line with fraud trends and patterns it is aware of. The Provider submits that as these trends can change all the time it cannot guarantee to stop every fraudulent transaction that takes place. The Provider submits that if a transaction does not appear to be in line with known trends it will not stop it.

The Complaint for Adjudication

The complaint is that the Provider wrongfully refused to refund disputed transactions carried out with the Complainant's debit card.

/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 8 April 2019, 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.

A submission dated 1 May 2019 from the Provider and a submission dated 8 May 2019 from the Complainant, were received by this Office after the issue of the Preliminary Decision to the parties. These submissions were exchanged between the parties and an opportunity was made available to both parties for any additional observations arising from the said additional submissions. I have considered the contents of these additional submissions together with all the evidence and submissions for the purpose of setting out the final determination of this office below.

The issue to be determined is whether the Provider wrongfully refused to refund disputed transactions carried out with the Complainant's debit card.

The Provider states that its "*Fraud Team had some reservations during the initial fraud investigation which was raised as a result of the Complainant's telephone call on 2 March 2017. The Bank was concerned about the unusual cash lodgement of €7,475 to the Complainant's account on 1 March 2017, which coincided with the date of the first alleged fraudulent transactions. The credit balance on the Complainant's account, before this lodgement was €4,586.85. The credit balance on the Complainant's account, after this lodgement, was €12,061.85. These funds were available to withdraw from the account as cleared funds. This cash lodgement, which the Bank again stresses was out of the norm for the customer based on the historic transactions on his account, ultimately had the effect of substantially increasing the amount and value of transactions which the Complainant has alleged as being fraudulent*".

/Cont'd…

The Provider in its submission to this Office dated 1 May 2019 states that "*This pattern of behaviour is in line with current fraudulent trends where a customer pays in a large sum of money into the account prior to an alleged fraud being perpetrated*".

The Provider also submits that the Complainant's Daily Withdrawal Limit for ATM transactions was €750.00 per day. The Provider submits that there are two instances between 1 March 2017 and 2 March 2017 where this amount, or an amount close to it, was withdrawn. The Provider states that "*on 1st March 2017 a withdrawal of €730 was made and on 2nd March 2017 withdrawals of €600 and €150 were made. Similarly on 8th March 2017, withdrawals of €150 and €600 were made. On 9th March 2017, via United Kingdom, Sterling amounts with Euro equivalents - €709.71 and €35.51 were made*". The Provider goes on to state that "*Withdrawing up to the maximum Daily Withdrawal Limit is also a known fraud trend*".

The Provider submits that despite such reservations, a decision was made to refund the Complainant's account in the sum of €2,216.03, which was credited on 9 March 2017.

In response, the Complainant submits that he has been a customer of the Provider since 2004, and "*in those 13 years of banking with [the Provider], I had lodged and withdrawn thousands of euros, so [its] claim is baseless that the deposit of €7,475.00 was out of normal transactions*".

The Provider states that "*While we are not disputing that the Complainant may have "lodged and withdrawn thousands of euros" on his account since that time, the point the Bank wished to make is that the lump sum lodgement of €7,475.00 which the Complainant credited to his account on 1 March 2017 was out of the norm for the type of transactions which the Complainant conducted on his account prior to that date*".

The Provider, in its submission dated 1 May 2019, states that "*The first alleged fraudulent transaction (on Card ending 0820) in the amount of €730 took place on 1st March 2017 at [the Provider's named branch]. It is considered very coincidental that the Complainant would be shoulder surfed so soon after paying in such a large amount of money (€7,475) into his account*". The Provider goes on to state that "*The Card activity matches what the Bank identifies with 'sold' accounts or collusion where multiple instances of incorrect pin are seen closely followed by correct pin being entered being entered. This does not fit with the pin having been obtained as a result of shoulder surfing*".

Regarding the first fraud investigation, the Provider submits that the Complainant advised its agent that while he was at the ATM, a "dodgy guy" asked him for directions. The Provider submits that the Complainant did not appear to be too concerned about this and advised its agent that he was careful to cover the ATM keypad in order to keep his PIN secure. The Provider states that "*During the course of the telephone conversation on 2 March 2017, the Complainant advised the Bank's agent that he could not find his wallet, which contained his DebitCard, Driver's Licence and College Identification*". The Provider goes on to state that "*in relation to what had happened to his DebitCard, this differed from what the Complainant initially told the Bank's agent at the beginning of the telephone call, i.e. that his card had*

/Cont'd…

been "caught in Bank" the previous night, which the Bank considers he meant that the DebitCard was captured in an ATM on the night of 1 March 2017. The Bank has not received any clarification from the Complainant in relation to these differing versions of events as to what actually happened to his DebitCard ending 0820".

The Provider states that "*If, as the Complainant appears to have implied, shoulder surfing did occur while he was at the ATM… on the night of 1 March 2017, this would not necessarily have resulted in the Complainant's Card being stolen at that time. Indeed, the Complainant has confirmed that he successfully withdrew €20 using his DebitCard, ending 0820, at that point*".

In response, the Complainant states the following:

> *"the bank claimed that Complainant advised the bank's agent that his ATM Card was "Caught in the Bank". Which the bank claimed that I meant that the Debit Card was capture[d] in an ATM on the night of 1 March 2017. This is [a] fabrication and a lie on bank's behalf, I had never tried [to] imply to the Bank's agent that my Debit card has caught in the machine… Every time I spoke to bank's representative I had repeated my incident and nowhere in my conversation with the bank's representative they gave me an impression that they misunderstood me.*
>
> *I was very clear in my statement over the phone and in all my correspondence with the bank that on [a named street] that night I withdrew 20 euro from the ATM and as always I was very cautious and protected while entering my pin, after I withdrew I put my card back into my wallet and in my wallet I had (Debit card ending 0820, driver's licence, student ID) as I turned back there was a guy behind who asked me some direction.*
> *This is a bank's dirty tactic to twist the situation by claiming that I had never [given it] any clarification on this issue, I had never claimed or [tried] to imply at the first place that my Debit Card (ending 0820) was "captured or caught in the ATM."*

Recordings of the telephone calls between the Complainant and the Provider have been provided in evidence.

I note during the telephone conversation on 2 March 2017 the Complainant, in relation to his debit card, stated that "*I think I lost it last night*". It is unclear from the telephone recording whether the Complainant went on to state that "*someone got call from the Bank*" or "*someone got card from the Bank*". However, I am of the view that the Complainant did not state that his card had been "*caught in Bank*". I also note that the Complainant went on to confirm that he could not find his wallet, which contained his college ID, driver's licence and debit card.

I note the following conversation between the Provider's representative and the Complainant during the telephone call on 2 March 2017:

Complainant: "*There was a guy at the back of me he asked directions when I was at the ATM*."

/Cont'd…

Provider: "*You think you've been pickpocketed?*"

Complainant: "*I could, yes cause the guy looked a bit dodgy… when I was... taking my 20 quid out he was asking for directions*."

Provider: "*Did he manage to get a look at your PIN when you entered it?*"

Complainant: *"I don't know, I don't know, I tried my best to block everything you know but"*

The Provider also states, in its submission dated 1 May 2019, that "*On a close review of the transactional history on the Complainant's account, the vast majority of transactions were 'Card Transactions', typically for online purchases, mobile telephone top-ups [name redacted], service station purchases [name redacted], grocery stores [name redacted] and leisure activities [name redacted]. Also, the Complainant used his Card to pay regular bills*". The Provider goes on to state that "*It was very unusual for the Complainant to use his Card to withdraw money from ATM machines, as was the case when he withdrew €20 from [the Provider] on the night of 1 March 2017 when he claims the issue with his Debit Card arose*".

The Provider submits that following the first fraud claim made by the Complainant, its agent cancelled the Complainant's debit card ending in '0820 on 2 March 2017 and a replacement card was ordered for the Complainant on that same date. The Provider states "*Consequently, the replacement DebitCard ending 1873 was dispatched to the Complainant's correspondence address on 3 March 2017*".

The Complainant submits that the Provider was fully aware that on 1 March 2017 his PIN for his debit card ending in '0820 had been compromised "*but [it] still ignored that fact and didn't issue the new Debit Card ending 1873 PIN*".

The Provider submits that following its process regarding advice of Lost and/or Stolen Card, its agent immediately cancelled the Complainant's DebitCard ending '0820 and ordered a replacement card for him (card ending '1873), advising that it would be sent to him in 4-7 days. The Provider submits that its agent confirmed the Complainant's correspondence address for this purpose. The Provider submits that the card ending in '0820 was replaced with card ending in '1873, which was posted to the Complainant at the address which he confirmed to its agent was his correspondence address.

The Provider submits that by replacing Card ending in '0820, that card was immediately invalidated and could no longer be used, regardless of whether or not the Complainant's PIN for Card ending '0820 was disclosed to another party. The Provider states that "*This explains why there was no need to issue the Complainant with a replacement PIN on the replacement card ending 1873*".

The Provider submits, in its submission dated 1 May 2019, that the normal/usual pattern of transactions on the Complainant's account evidences his weekly dependency on his account to cover his cost of living expenses. The Provider states that "*During the period between the cancellation of his initial card (ending 0820) on the 2nd March 2017 until he received the second replacement card (ending 4646 (with the first transaction being applied on the 20th*

/Cont'd…

March 2017), we would question why the Complainant didn't have the need to visit [a Provider] branch to make any cash withdrawals to cover his usual living expenses based on the usual account transaction history. The Bank's teller would have been in a position to assist the Complainant with over the counter cash withdrawals from his account, despite any inability on his part to present valid identification. This could have been achieved by following internal security procedures which would have enabled our staff to confidently verify the Complainant's identity".
The Provider goes on to state that it "*questions how the Complainant managed to pay bills and expenses during that period or have funds to cover his day to day costs of living without making any cash withdrawals or online payments from his account during the prolonged period of the alleged fraudulent transactions, 1st to 10th March 2017 until he received the second replacement card (ending 4646)*".

In response, the Complainant submits that he had friends and family with him at that time to help him on a week to week basis. The Complainant states that "*This is a blunt try from the bank's side to make everything seem blur. But the FACT is bank failed to protect my monies, Bank system failed to raise any alarm on those fraudulent transactions. And now they are trying to blame on someone else for their failure*".

The Provider submits that the Complainant telephoned the Fraud Department on 10 March 2017 and advised that he had not received his replacement debit card (card ending in '1873). The Provider submits that the Complainant's account transactions were checked and it was established that the debit card ending in '1873 was used for transactions, which the Complainant claimed were not made by him, and are the subject of this complaint. The Provider submits that its agent advised the Complainant that the debit card ending in '1873 had been posted to his correspondence address. The Provider states that "*Because the Complainant stated the transactions were not made by him, and as the Complainant confirmed to the agent that his post is sent to a communal mailbox, the possibility that the replacement DebitCard was intercepted from the Complainant's post-box and used by a fraudster was discussed*".

The Provider, in its submission dated 1 May 2019, submits that during the telephone call on 10 March 2017, the Complainant said that he got a text nonfiction from the Bank stating that the replacement card was dispatched on the previous Saturday, which would be 4 March 2017. The Provider submits that the replacement card ending in '1873 was reordered on Thursday 2 March 2017 and dispatched on Friday 3 March 2017.

The Provider submits that its replacement Debit Cards are issued by an outsourced company based in London, and that there is a Service Level Agreement for the generation and dispatch of these cards, which was adhered to in the case of the Complainant's replacement card. The Provider states "*Once the Card is dispatched in the post, in this case Royal Mail in the United Kingdom until it reaches Republic of Ireland, the actual delivery date relies on the efficiency of the applicable postal service. It is for this reason that Bank staff cannot definitively state when a Card will arrive at the correspondence address destination and therefore we typically advice that delivery will be within 5 working days*". The Provider goes on to state that "*Consequently, the Bank strongly contends that someone would have to check the Complainant's mailbox on a daily basis in order to successfully intercept the post*

/Cont'd…

and get access to his replacement Debit Card. The Bank considers that the coincidence of a random interception of the Complainant's replacement Debit Card by the same alleged 'shoulder surfer' to be highly unlikely".

I note that the telephone conversation between the Provider's representative and the Complainant on 10 March 2017 went as follows:

Provider: "*Is it a shared mail box?*"

Complainant: "*Yes, it's a communal mailbox*"

Provider: "*Yes, so it's likely been then that the cards been sent there and someone's intercepting it cause its happened twice at your address*"

…

Provider: "*What I am saying that if it's getting sent to your address it's likely that someone who knows about this or someone at your address*"

…

Complainant: "*I never received the new PIN, how could they have the new PIN*"

Provider: "*So it's not a new PIN the new PIN wasn't issued it's just the new card that was issued*"

…

Provider: "*So while the PIN was compromised, with a new card if you have the card… you get the card they couldn't' use it. So what's obviously happened here, and I've seen it happen in the past, it's a flat, it's a shared mailbox so someone is accessing your mailbox*".

The Provider's representative confirmed that she was cancelling the card ending in '1873 and going to get the new one issued and sent to the branch. The Complainant confirmed the nearest branch, and the Provider's representative confirmed that she would not get anything sent to the Complainant's home address. The Complainant requested a new PIN to be sent out, and questioned why one was not sent with the last card.

The Provider's representative stated:

> "*If your card became compromised and there's been someone looking over your shoulder at an ATM we don't really need to cancel the PIN we just need to cancel the card and the PIN can normally remain the same but it looks like it's either… unlucky that its happened to you again by someone else or the same people have intercepted your post so it's unlikely that this does happens twice so that's why we wouldn't have needed to have cancelled the PIN, the PIN could have remained the same… Ok I am going to do it for you now because of what's happened twice… I'll issue a brand new card and a brand new PIN."*

The Provider submits that card ending in '1873 was replaced with card ending '4646, actioned as result of the telephone call between its agent and the Complainant on 10 March 2017. The Provider submits that it was during this telephone call that the Complainant was

/Cont'd…

advised by its agent that it would send the replacement Card (card ending in '4646) to its named branch. The Provider states that "*It appears that this was recommended by the Bank's agent following the Complainant's claim that he had not received the replacement Card which was ordered on 2 March 2017 and an ensuing discussion regarding the possibility that the Complainant's post was intercepted by a fraudster from the Complainant's communal post-box*". The Provider goes on to state that "*The Bank concedes that replacement Card, ending 4646, was not sent to [named] branch for Complainant's collection, but rather was posted to the Complainant's correspondence address in error. We wish to apologise to the Complainant for this oversight*".

The Provider goes on to state that "*it is vital to note that the Complainant has not raised with the Bank, or through the office of the Financial Services Ombudsman's Bureau, any alleged fraudulent transactions occurring as a result of use of Card ending 4646. The alleged fraudulent transactions occurring on the Complainant's Current Account, being the subject matter of this complaint, all occurred on Card ending 1873. That card (ending 1873) was posted to the Complainant's correspondence address, as agreed with him during the telephone conversation with the Bank's agent on 2 March 2017*".

The Complainant submits that when he asked the Provider "why *the banking system didn't raise any alarm when these transactions took place, I was told by the bank because of the pattern of these transactions the system didn't consider them as fraudulent*". The Complainant has submitted two "*TEXT ALERTS*" from the Provider "*showing that Bank System informed me straight away and clocked the debit card when my debit card/Pin was compromised initially".* The Complainant states that "*As you will notice that all six of these fraudulent transactions [were] carried out with the same pattern and in a short period of time and these were large amounts totalling [€]12,030.84. Furthermore… one massive transaction of €9,943.73 was made at POS in the UK, but the bank system failed to raise any Alarm/Alerts on this occasion*".

The Complainant submits that the Provider should have been more cautious as one of the transactions was a large one and was carried out abroad while he was in college in Ireland at the time. The Complainant states that "*I believe the customers contact their banks in advance before going to make any huge single transaction abroad or [at] home, otherwise the bank verifies it by sending text to confirm if it's the genuine transaction*". The Complainant also states that "*I was told during one of the phone calls by the fraud department operatives that the bank should have sent me text alerts but did not as the system was not functioning properly, as an excuse by the bank for being negligent*".

The Complainant has submitted a copy letter from his college confirming that he was in college on 9 March 2017, which I note states:

> *"I would like to confirm that [the Complainant], is a student on the full time programme [named course].*
>
> *Our records show that this student was in attendance at a [named lecture] which took place during a laboratory session scheduled 2-4pm on Thursday, 9th March."*

/Cont'd…

The Provider submits that it cannot advise its customers every time a transaction is presented for payment. The Provider submits that its Fraud Team consistently monitor fraud developments and fraud patterns occurring which affect its customers or have the potential to affect its customer. The Provider states that "*However, the Bank can only monitor accounts in the context of known fraud trends, identified as a result of ongoing and vigilant fraud intelligence, of which the Bank is aware at a particular point in time*". The Provider goes on to state, in its submission dated 26 September 2017, that "*Based on current Fraud intelligence and ongoing monitoring of developments in the area of fraud, the Bank contends that, at time of writing this report, it is not possible to clone or replicate an authentic Chip on Cards. This fact further supported the conclusion that the genuine Debit Card (ending 1873) together with correct PIN, were used to effect payment on the disputed transactions*".

In its submission dated 1 May 2019, the Provider submits that there were regular online logons made by the Complainant via his secure Internet Banking service throughout the period of the alleged fraudulent events. The Provider states that "*the frequency and timings of online activity after the point in time when the Bank had cancelled his card on 2nd March 2017, until the Complainant telephoned the Bank to say he never received the replacement card on 10th March 2017, is extremely curious in circumstances where the Complainant was not actually carrying out any online transactions e.g. payments or transfers… so it would appear as if he was monitoring the account very closely throughout each day*".

The Complainant submits that he was advised by "*customer services my monies would be refunded, now after I have made numerous telephone calls, I have been advised this will not be the case. The bank has offered no plausible reason as to why the refund has been refused*".

The Provider submits that during the telephone call on 10 March 2017, its agent took the Complainant through a refund claim form for the disputed transactions occurring on his account as a result of use of debit card ending in '1873. The Provider submits that the Complainant was advised that this fraud claim would be passed to the relevant Investigations Team to investigate, and that he would have an update from the that team within 5 working days. The Provider states that "*No promises regarding impending refunds were given to the Complainant at any point. This is because the disputed transactions had to be investigated before an outcome was reached and before a decision on the fraud claim could be communicated to the Complainant… the Bank categorically disputes the Complainant's claim… that he was advised by the Bank that his monies would be refunded".*

I note that during the telephone conversation between the Provider's representative and the Complainant on 10 March 2017, the Provider's representative confirmed that as the transactions were carried out by chip and PIN and were of a large value the case would need to go for an assessment. The Provider's representative stated that "I *can't really comment on it. It is likely you are going to get the money back… but obviously I can't say for definite there as it's just been passed over to them*".

The Provider states that it "*wishes the timeline of the alleged fraudulent transactions on 1 March i.e. being 3 and 22 minutes after the Complainant's ATM withdrawal of €20 at 21.34pm at [a named location in Dublin City Centre], together with the location of one of these transactions at [another named location in Dublin City Centre], to be noted. These facts*

/Cont'd…

do not give credence to the theory that the same person who possibly shoulder-surfed the Complainant on the night of 1 March 2017 while asking for directions (and possibly saw the PIN for Card ending 0820) could establish the home address of the Complainant a number of days later, enable interception of his replacement Card (ending 1873) for use with the Complainant's PIN (which was unchanged) and allow the fraudulent transactions, now subject of this complaint, to occur. The Bank questions how would the same individual, who may possibly have seen the Complainant's PIN on the night of 1 March 2017 (albeit the Complainant advised the Bank he was careful to conceal his PIN), could have knowledge of the Complainant's home address and get access to the Complainant's replacement card, which was posted to his home address 3 days after the Complainant was at the… ATM on 1 March 2017. The Bank considers such a scenario highly unusual and ultimately unlikely".

In response, the Complainant states that "*As I explained to the Bank over the phone and in my letters to [it], that my WALLET was stolen and in my wallet I had debit card (ending 0820) my college ID and also my driver's licence with my photo and my current house address. And I also had mentioned… that I have a communal Post box in our house, we don't have separate Post Boxes for each flat*".

The Provider states that it "*cannot find any record in the Complainant's dealings with the Bank to show that he advised the Bank that his home address was noted on his driver's licence and/or in his wallet which he alleges were stolen on the night of 1 March 2017*". I note that there is no evidence that the Provider sought this information from the Complainant.

The Provider submits, in its submission dated 1 May 2019, that in the Complainant's telephone call of 2 March 2017, he told its agent that he was in an exam, which was due to finish at 5pm. The Provider states that "*However, he said that he had finished the exam early and he made a call-back to the Bank regarding his account, which resulted in the first fraud claim being raised. Please note that despite the Complainant stating that he was sitting an exam up to 17:00 that date, he logged into his… Internet Banking account at the following times during that day: 14:19PM, 16:21PM (and later at 21:42PM). These afternoon logons do not give credence to the Complainant's contention that he was in an exam when one of the disputed transactions occurred on Card ending 0820*". The Provider submits that on the afternoon of the Complainant's exam a transaction with a merchant was carried out at 12:50pm for €600. The Provider states that "*this raises serious credibility issues on the Complainant's part*".

The Provider goes on to submit that the Complainant only contacted it at 16:50pm on 2 March 2017 to notify of the alleged theft of his wallet "*which he stated contained his debit card, Driver's Licence and College Identification*". The Provider states that "*If, as he has stated, the Complainant was taking an examination on 2nd March 2017, the likelihood is he would have needed his College Identification for examination purposes*". The Provider goes on to state "*That being the case, we submit that knowledge of the absence of his wallet and its contents ought to have been known to the Complainant earlier than when he contacted the Bank at 16:50PM on the 2nd March 2017*".

/Cont'd…

The Complainant has submitted screenshots from a Facebook page and his college timetable, which he submits "*prove that it was the "MOCK [redacted] TEST" for a module called [redacted] which doesn't require any College ID and we student[s] are able to go out of the [room] if necessary. (like answering a phone call, in that case a call from [the Provider]. [Redacted] has a Facebook group account where the student[s] from my class were added in a group*". The Complainant goes on to state that "*As you can clearly see my classmate posted a reminder on Facebook about a mock [redacted] test for [redacted] on (2nd march 2017 Thursday) the day the Bank [was] surprised [ ] how I managed to sit in without a college ID. A student doesn't require any ID to sit in a mock [redacted] test*".

The Complainant submits that the class timetable "*Clearly shows that the Module [redacted] falls on every Thursday between 2:00pm to 4:00pm from 26th January 2017 til 4th May 2017*".

Given that the Complainant informed the Provider during the telephone call of 2 March 2017 that his ID including his student card and Driver's Licence were also "missing", I am of the view that it would have been prudent for the Provider to ask the Complainant if he wanted a new PIN with his new Card.

The Provider submits that the following disputed transactions are alleged by the Complainant to be fraudulent:

Date of Transaction	Date applied to Account	Transaction Type	Amount
8 March 2017	9 March 2017	Cashline/ATM Transaction	€ 150.00
9 March 2017	9 March 2017	Cashline/ATM Transaction	€ 709.71
9 March 2017	9 March 2017	Cashline/ATM Transaction	€ 35.51
8 March 2017	10 March 2017	Cashline/ATM Transaction	€ 600.00
9 March 2017	10 March 2017	Point of Sale/DebitCard	€9,943.73
10 March 2017	10 March 2017	*Cashline/ATM Transaction	€ 591.89
		Total Disputed Transactions	**€12,030.84**

The Complainant states that "*I would like to show you the unprofessionalism on banks behalf. The bank claim [ ] that there were five fraudulent transactions took place total of 11,438.95, in fact there were total six fraudulent transactions took place total of 12,030.84… [it] didn't include the fraudulent transaction total of 591.89 which took place on 10th March at the ATM in the UK. This shows the careless attitude towards [its] customers and unprofessionalism on bank's behalf*".

The Provider submits in relation to the transaction of €591.89 this transaction had not yet been applied to the Complainant's account when the telephone call of 10 March 2017 occurred at 13.36pm. The Provider states that "*As such, it had not been identified during the Complainant's telephone call with the Bank's agent and therefore was not included in the list of alleged fraudulent transactions recorded with the Complainant during the course of the telephone call*". The Provider submits that as a result, this transaction was not included in its investigation and ultimately was not included in the transactions which it declined to refund. The Provider states that "*Following on from this, the Bank's letter of 23 March 2017 referred to a decline of fraud claim in the sum of €11,438.95 (being €12,030.84 minus €591.89). For the purpose of clarity… the Bank's decision to decline the fraud claim currently*

/Cont'd…

the subject of this dispute, extends to include a decline of transaction on 10 March 2017 in the amount of €591.89".

The Provider submits that on 10 March 2017 its Fraud Department set up a new Fraud Claim, and on 17 March 2017, a decision was taken to "*Manage Out*" the Complainant's account and provide him with 60 days' notice of account closure. The Provider submits that a letter was issued to the Complainant on 20 March 2017 providing him with 60 days' Notice to Close Accounts held with it, and the Complainant's current account was subsequently closed on 22 May 2017.

The Provider has obligations pursuant to the European Communities (Payment Services) Regulations 2009 (hereinafter referred to as the "2009 Regulations"). I am satisfied that the relationship between the parties is governed not only by the contractual agreement between them, but also by the statutory provisions of the 2009 Regulations. The 2009 Regulations implement a set of rights and obligations where a consumer engages a Payment Service Provider, such as the Provider in this case, to carry out a Payment Service (i.e. "*enabling cash withdrawals from a payment account")* by means of a Payment Instrument (i.e. physical devices (such as cards) and/or a set of procedures).

The Regulations set out how a transaction using a card can be carried out with consent by the accountholder and also how such a transaction is classed as authorised or unauthorised. Specifically, Regulation 68 of the 2009 Regulations states that:

> *68. (1) A payment transaction is authorised only* ***if the payer concerned has consented to its execution.*** *A payer can authorise a payment transaction before or, if agreed between the payer and the payment service provider concerned, after the execution of the payment transaction.*
>
> *(2) Consent to execute a payment transaction or a series of payment transactions is valid only if given in a form agreed between the payer and payment service provider concerned.*
>
> *(3)* ***In the absence of consent, a payment transaction is unauthorised.***
>
> *(4) A payer may withdraw his or her consent at any time before the time of irrevocability under Regulation 82. A payer may withdraw his or her consent to execute a series of payment transactions with the effect that any future payment transaction is unauthorised.*
>
> *(5) The procedure for giving consent shall be as agreed between the payer and the payment service provider."* (emphasis added).

The Provider states that its "*investigations unequivocally show that the Chip and PIN were used to authorise the disputed transactions and furthermore, current Fraud Intelligence show that Chip Cards cannot be cloned. Therefore, the individual who authorised the transactions had possession of both the Chip and PIN in order to secure the disputed payments*". The Provider also states that "*Although [the Complainant] states that he did not*

/Cont'd…

share his Card or PIN with anyone; that he did not write down his PIN/have it noted in his wallet which he states he lost with his DebitCard contained within, due to the… information known to the Bank and gathered during investigation, the only plausible explanation of how the Complainant's Card and PIN were compromised was that the Complainant authorised the transactions himself using his Card and PIN, or that he allowed somebody else to do so, the latter scenario being a direct contravention of the… Terms and Conditions of Card Use".

Regulation 70 of the 2009 Regulations places a number of obligations on customers. It provides the following:

> *"70. (1) The obligations of a payment service user entitled to use a payment instrument are-*
>
> *(a) of using the payment instrument in accordance with the terms governing its issue and use, and*
>
> *(b) of notifying the payment service provider that issued the instrument, or an entity specified by that payment service provider, **without undue delay** on becoming aware of the loss, theft or misappropriation of the payment instrument or its unauthorised use.*
>
> *(2) For the purposes of paragraph (1)(a), a payment service user shall, as soon as he or she receives a payment instrument, **take all reasonable steps to** keep its personalised security features safe."* [emphasis added]

It is therefore necessary for the Complainant to use his debit card in compliance with the terms and conditions agreed with the Provider. The Provider has submitted a copy of the terms and conditions relating to the Complainant's visa debit card at the time of the disputed transactions. The Provider states that "*the Complainant failed to adhere to these Terms and Conditions and that is the basis of the Bank's decision to decline a refund of alleged transactions totalling €12,030.34".*

I note that Condition 2 of the terms and conditions states, among other things, the following:

> *"2 The card*
> *…*
> *2.2 You (and any additional cardholder) must do the following:*
> - *Sign the card when You or the additional cardholder receive it.*
> - *Keep the card secure at all times and not allow any other person to use it*
> - *On receiving the PIN advice slip memorise the PIN and then immediately destroy the PIN advice slip.*
> - *Never write down the PIN in any way which could be understood by someone else.*
>
> *Failure to follow the above procedures may affect your liability for unauthorised payments as set out in Condition 7.2"*

/Cont'd…

The Provider submits that Condition 9, underneath the heading "*A General Account Terms and Conditions*" states:

"9 Security Procedures

9.1 You must keep your Security Details secret and take all reasonable precautions to prevent unauthorised or fraudulent use of them.

9.2 You must not disclose your Security Details to any other person or record your Security Details in any way which may result in them becoming known to another person.

9.3 Please note that after initial registration or enrolment We will never contact You, or ask anyone to do so on our behalf, with a request to disclose your Security Details in full. If You receive any such request from anyone (even if they are using our name and logo and appear to be genuine) then it is likely to be fraudulent and You must not supply your Security Details to them in any circumstances. You should report any such requests to us immediately.

9.4 If You suspect someone knows your Security Details or there is unauthorised use of your Account You must contact us immediately at our branch or locall… If You fail to do so, You may be liable for unauthorised Transactions up to €75 on your Account arising from the lost or stolen Security Details or where You have failed to keep your Security Details safe. If You acted fraudulently or intentionally, or with a gross lack of reasonable care failed to comply with your obligations in this paragraph or breached these Terms and Conditions, the limit of €75 will not apply and You may be liable for the full amount of the unauthorised Transaction on your Account.

9.5 You are not liable for any unauthorised Transactions made using your Security Details after You have notified us in accordance with condition 9.4 of this Section A above unless You acted fraudulently.

9.6 See Condition 8 of Section E for details of your responsibilities relating to your Security Details where You have a debit card on your Account."

Condition 3 of Section E of the Terms and Conditions states:

"E. Debit Card – Conditions of Use

Using the card

3 Transactions

3.1 You must only use your card in accordance with these Terms and Conditions.

…

3.7 If a retailer or supplier of services accepts payment by your card, the use of your card will have the effect of guaranteeing the payment and We will be obliged to pay the sum due to the retailer or supplier.

…

3.13 You will have to pay all amounts charged to your Account by your card, even when the details on the sales voucher are wrong or where no sales voucher is signed, if it is clear that You or any additional cardholder has authorised the transaction.

…

/Cont'd…

3.15 A transaction will be regarded as authorised by You or an additional cardholder and You give your consent to the transaction where You (or the additional cardholder):

(a) authorise the transaction at the point of sale by following whatever instructions are provided by the merchant to authorise the transaction, which may include:

(i) entering the PIN or providing any other security code;

(ii) signing a sales voucher;

(iii) providing the Card Details and/or providing any other details requested; or

(v) waving or swiping the card over a card reader.

(b) insert the Card and PIN and make a request for a cash withdrawal or a third party payment from an ATM or at a bank counter;

(c) orally or in writing provide the Card details to the Bank or request a transfer from the Account.

3.16 Notwithstanding that You must always use your PIN, if You sign for goods and/or services You consent to the transaction."

Condition 7 of Section E of the Terms and Conditions sets out the following:

7 Liability

7.1 If the card is lost or stolen, or You suspect that someone knows the PIN, You must carry out the instructions set out in the Important Notice at the beginning of these Conditions.

7.2 If the card is misused before You tell us of its loss or theft or that someone else knows the PIN in accordance with Condition 7.1 above, You will only have to pay up to €63.49 for any misuse, unless You have acted fraudulently or unless You intentionally or with a gross lack of reasonable care, failed to fulfil your obligations in Condition 7.1 and Condition 3.1. If You act fraudulently or intentionally or with a gross lack of reasonable care fail to fulfil your obligations under Conditions 3.1 and 7.1, the above limit will not apply and You may be liable for all amounts which arise from any misuse.

7.3 You are not liable for any unauthorised transaction made using your card and/or PIN after You have notified us of the loss, theft, misappropriation or unauthorised use of your card in accordance with Condition 7.1 above and We will re-credit any such transaction made with your card after You have contacted us, unless You have acted fraudulently.

7.4 If the card is misused by someone who has it with your permission You will have to pay for all transactions carried out with the card by that person.

7.5 If someone carries out a fraudulent transaction using your card details on the Internet or by telephone or mail order You will not be liable for the fraudulent transaction provided You notify us without undue delay on becoming aware of the misuse.

/Cont'd…

7.6 Once We receive notice of the loss, theft or possible misuse, We will cancel the card. If the card is then found You must not use it. You must return it to us immediately cut in half through the signature box and magnetic strip, and if You have a chip card ensure the chip is cut in half.

7.7 You will not be responsible for any loss arising from misuse of a card if it has not been received by You.

7.8 We will not be liable if any party refuses to let You pay or withdraw cash with the card.

7.9 Subject to Conditions 7.2 and 7.13, We will refund You immediately on establishing that a transaction was not authorised or consented to in accordance with Condition 3 which transaction was debited to your Account by crediting your Account with the amount and any interest lost due to the unauthorised transaction.

…"

The Provider states, "*The Complainant has stated that he did not authorise these transactions. However… the Bank wishes to refer to the obligations by the Complainant in keeping his security details and Card safe, not sharing these with anyone and not acting with "a gross lack of reasonable care" which would result in his inability to fulfil his obligations under the Bank's Terms and Conditions of Card Use*".

Regulation 74 of the 2009 Regulations deals with "*Payment service provider's liability for unauthorised payment transactions*" as follows:-

"74.(1) In the case of an unauthorised payment transaction, the payer's payment service provider shall, if the payer concerned has given notice in accordance with Regulation 72 refund to the payer immediately the amount of the transaction and, if necessary, restore the debited payment account to the state it would have been in had the transaction not taken place.

..."

Regulation 74 must be read in light of the terms of Regulation 75 of the 2009 Regulations, which provides as follows:

"Payer's liability for certain unauthorised payment transactions.
75. (1) Despite Regulation 74, and subject to paragraphs (2) to (5), a payer shall bear the loss relating to unauthorised payment transactions on the payer's account, up to €75 in total, if the transaction results from-

(a) the use of a lost or stolen payment instrument, or
(b) if the payer has failed to keep a payment instrument's personalised security features safe, its misappropriation.

(2) A payer shall bear all the losses relating to an unauthorised payment transaction if he or she incurred them by acting fraudulently or by failing,

/Cont'd…

intentionally or by acting with gross negligence, to fulfil one or more of his or her obligations under Regulation 70.

(3) A payer shall not bear any financial consequences resulting from the use of a lost, stolen or misappropriated payment instrument after giving notice in accordance with Regulation 70(1)(b), unless he or she has acted fraudulently.
..."

Regulation 73 of the 2009 Regulations provides the following:

"Evidence on authentication and execution of payment transactions
73. (1) If a payment service user denies having authorised an executed payment transaction or claims that a payment transaction was not correctly executed, it is for the payment service provider concerned to prove that the transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other error or failure.

(2) If a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider is not in itself necessarily sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or intentionally or failed, because he or she acted with gross negligence, to fulfil one or more of his obligations under Regulation 70"

The term "gross negligence" is not defined in the 2009 Regulations nor in the Parent Directive (Directive 2007/64/EC). Recital 33 of the Parent Directive states that:

"...in order to assess possible negligence by the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should be evaluated according to national law".

Under Irish law the concept of gross negligence was considered both by the High Court and the Supreme Court in the case of ICDL Saudi Arabia v European Computer Driving Licence Foundation Ltd [2011] IEHC 343; [2012] IESC 55. In that case a majority of the Supreme Court approved the High Court's test for gross negligence, namely *"...a degree of negligence where whatever duty of care may be involved has not been met by a significant margin."*

It is clear from the terms and conditions of the account that, in circumstances of theft of the card or PIN, that the account holder will only be liable for the first €63.49 for any misuse unless "*You have acted fraudulently or unless You intentionally or with a gross lack of reasonable care, failed to fulfil your obligations in Condition 7.1 and Condition 3.1".*
Regulation 75(1)(b) of the 2009 Regulations specifically notes that a cardholder must only pay up to the first €75.00 in total of any loss, if the card has been misappropriated where *"the payer has failed to keep a payment instrument's personalised security features safe".*
Clearly, it is therefore possible, according to the Regulations, for a cardholder to bear the

/Cont'd…

loss up to €75.00, even where they have failed in certain circumstances to keep the card's security features safe. However, Regulation 75(2) then sets the boundary of that protection, to exclude losses where "*he or she incurred them by acting fraudulently or by failing, intentionally or by acting with gross negligence, to fulfil one or more of his or her obligations under Regulation 70*".

It is clear from the wording of Regulation 75 of the 2009 Regulations that differing degrees of responsibility upon cardholders are envisaged in relation to losses incurred through a failure to keep their card's security features safe. In order for the Provider to place liability upon the Complainant I consider that in this instance it must be in a position to evidence, quite apart from the mere use of the Complainant's card and correct PIN, that the Complainant's loss was not simply due to his failure to keep the Chip card security features safe. The Provider must also be able to evidence that this failure was due to either the intentional or fraudulent acts of the Complainant, or due to his "gross negligence", as outlined in Regulation 75(2).

While it is clear from the use of the chip card and PIN that the person(s) who carried out the unauthorised transactions did come into possession of the Complainant's card and PIN, and that the use of the PIN together with the card may evidence that the Complainant failed to keep the security features of his card safe, I have no evidence before me to suggest that this was caused by the Complainant's intentional or fraudulent acts, or due to his gross negligence. As noted above Regulation 73(2) specifically provides that use of the PIN with the card "*is not in itself necessarily sufficient*" to prove that the payment transactions were authorised by the Complainant or that he breached the obligations of Regulation 70 by acting in an intentional or fraudulent manner or through his gross negligence.

In the Complainant's case the Provider has submitted that the Chip card and correct PIN were used to authorise the disputed transactions, and "*the only plausible explanation of how the Complainant's Card and PIN were compromised was that the Complainant authorised the transactions himself using his Card and PIN, or allowed somebody else to do so, the latter scenario being a direct contravention of the… Terms and Conditions of Card Use*".

On the balance of the evidence before me, I consider that the Provider has produced insufficient evidence upon which it would be reasonable to conclude that the Complainant had failed to fulfil his obligations under Regulation 70 of the 2009 Regulations such as to justify its decision to refuse to refund the remainder of the disputed transactions. Consequently, I accept that the Complainant was entitled to a refund of the transactions which he disputed in accordance with Regulation 75(1), and the Provider was obliged to immediately refund the Complainant the amount of the disputed transactions in accordance with Regulation 74(1), when the Complainant raised the matter March 2017.

Consequently, this complaint is upheld. I direct the Provider to refund the total amount of the transactions (totalling €12,030.84) to the Complainant less the sum of €63.49 for which he is liable pursuant to Condition 7.2 of the account terms and conditions. I also direct the Provider to make a compensatory payment of €500.00 to the Complainant to mark its failure to immediately refund the Complainant in accordance with its obligations as outlined in

/Cont'd…

Regulation 74(1) and its error of issuing card ending in '4646 to the Complainant's home address instead of the Provider's branch as agreed during the telephone conversation of 10 March 2017.

Conclusion

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

- Pursuant to ***Section 60(4) and Section 60 (6)*** of the ***Financial Services and Pensions Ombudsman Act 2017,*** I direct the Provider to refund the total amount of the transactions (totalling €12,030.84) to the Complainant less the sum of €63.49 for which he is liable pursuant to Condition 7.2 of the account terms and conditions. I also direct the Provider to make a compensatory payment of €500.00, 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 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

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