An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

Decision Ref:	2021-0481
Sector:	Banking
Product / Service:	Current Account
Conduct(s) complained of:	Handling of fraudulent transactions
Outcome:	Substantially upheld

LEGALLY BINDING DECISION
OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

This complaint concerns the Provider's handling of disputed transactions on the Complainant's accounts.

The Complainant's Case

The complaint is that the Provider was negligent in that it permitted a number of unauthorised transactions to be carried out on the Complainant's accounts.

The Complainant states that he telephoned the Provider prior to **13 June 2017** to place a block on his debit card (linked to current account ****5588), and that the Provider's staff member advised him that the card was blocked. He states that fraudulent activity began on **15 June 2017**, at a time when he was away on holidays. The Complainant contends that the Provider failed to process his instructions by failing to place a block on the debit card, thereby permitting fraudulent transactions to be carried out on the account.

The Complainant states that his account ****5588 had a zero balance at the time he attempted to place a block on the debit card associated with it. He contends that as a result of further failures on the part of the Provider, funds were fraudulently transferred from another current account he held with the Provider (****7045) into account ****5588. These funds were then dissipated, fraudulently. The Complainant contends that the Provider failed to ask the appropriate security questions and he asserts that the contents of a number of recorded telephone calls to the Provider, made by the person(s) who allegedly carried out the fraud, will substantiate this complaint.

The Complainant contends that the Provider failed to monitor or 'flag' what he describes as unusual banking activity on his accounts. He points to the level of withdrawals that took place in the space of one week – totalling over €10,000 – a level of activity which he states would have been out of character for him. By way of example, he states that he had previously been required to answer a number of security questions when booking a flight for €700.

The fourth element of the complaint is that the Provider permitted two cheques to be lodged to his accounts (one into each account), which were returned unpaid and then re-presented on a number of occasions, thereby permitting his account balance to be temporarily and artificially inflated with uncleared funds and allowing the purported fraudster to withdraw greater sums of money from his current accounts, before the cheques were returned unpaid.

In addition to the above matters, the Complainant states that since the occurrence of the above events, the Provider failed to provide an adequate level of service in relation to his complaints. He says he felt treated like a criminal and ultimately the Provider terminated the bank/customer relationship with the Complainant and his accounts were closed, leaving a debit balance which the Complainant states is a result of the frauds to which he fell victim.

The Complainant would like his current accounts restored and reinstated to their “pre fraud” balances.

The Provider's Case

The Provider states that there is no record of any contact from the Complainant prior to 13 June 2017 seeking to have his debit card (card ending 7799) blocked (or to report it stolen or lost) in the manner suggested by him.

The Provider states that on **9 June 2017** the Complainant advised it he was in Switzerland and that he could not find his debit card. The Provider offered to re order a card and send it to his home address (as per its records) or to send it to his local branch, but the Complainant declined both offers. The Complainant wanted a card posted to his friend's address in Switzerland but the Provider advised that it could not do so as this would be outside the Provider's process for posting cards. The Provider states that during this phone call the Complainant was advised that he had a credit balance of just under €7,000 in his account ****7045. The Provider states that the debit card associated with this account (card number ending 9551) was consistently being used both before and after this phone call. The Provider states that when the Complainant was transferred to the department for lost and stolen cards he ended the telephone call.

The Provider contends that the fund transfers at issue in this complaint were carried out using the Provider's internet banking facility. It explains that in order to effect these transactions, the internet platform requires a customer number; a card number; a PIN; and a password.

/Cont’d…

It states that *"it was only the Complainant who could have made these transfers"*, or if it was not the Complainant, then the Complainant must have been grossly negligent in allowing a third party to access all of the information required to carry them out.

The Provider will not divulge its specific anti-fraud measures, however it confirms that it has various strategies in place to try to stop frauds being perpetrated on customers' accounts. It states that the caller on the telephone call of **15 June 2017** answered all security questions correctly and the Provider was therefore satisfied that its internal procedures were follows. The Provider once again notes that if a third party was in possession of the information necessary to answer those security questions, this could only have happened by reason of the gross negligence of the Complainant.

The Provider rejects the criticisms levelled at it for its handling of the cheque lodgments. In relation to the cheque for €4,865.00 to account ****7045, it contends that there was no adverse effect to the balance to that account by reason of the cheque being lodged and returned unpaid. In short, it contends that there were no disputed debits on the account while it was awaiting clearance, so a temporary inflation of the balance with uncleared funds did not make any difference. It notes that this lodgment was made in branch on **19 June 2017** by a person who would have been in possession of the Complainant's bank account number and sort code, and the cheque (made out to the Complainant).

In relation to the lodgment(s) of cheque for €3,998.00 to account ****5588, the Provider agrees that these credits exacerbated the situation, however it rejects criticism of its actions in this regard. This cheque was also lodged on **19 June 2017** in branch (albeit a different branch to the other cheque). Again, the person who lodged it would have been in possession of the Complainant's bank account number and sort code, and the cheque was made out to the Complainant.

Both cheques were lodged using fast lodgment boxes and thus the person lodging them avoided contact with branch staff.

The Provider notes that transactions to the value of €3,971.14 were carried out on the account whilst this cheque was awaiting clearance. The final overdrawn balance is €4,076.31.

The Provider states that it carried out an appropriate investigation prior to declining the Complainant's claim for a refund of the disputed transactions, and that it has dealt with the Gardaí in the appropriate manner. The Provider also notes that it is entitled to close a customer's account without giving reasons, and it gave 7 days' notice of the closure of the Complainant's accounts on **27 June 2017**. Account ****5588 remains open as it has a debit balance as set out above.

/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 18 November 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.

Following the issue of my Preliminary Decision, the parties made the following submissions:

1. E-mail from the Complainant, together with attachment to this Office, dated 24 November 2020,

2. Letter from the Provider to this Office dated 11 December 2020.

3. E-mail from the Complainant to this Office dated 14 December 2020.

4. Letter from the Provider to this Office dated 21 December 2020.

Copies of these submissions were exchanged between the parties.

The Complainant advised this Office under cover of his e-mail dated 27 January 2021 that he had no further submission to make and that he is "*more than ready for the Ombudsman to adjudicate this matter*".

/Cont'd…

Having considered these additional submissions and all submissions and evidence furnished by both parties to this Office, I set out below my final determination.

In my Preliminary Decision I had detailed that the Complainant opened account ****5588 by filling out an application form dated **25 May 2017**. The Provider has, in its post Preliminary Decision submission, asked that it be noted that this account "*was not opened through the* [Provider's] *branch network, but rather it was opened via online banking*". The online application was made on **11 May 2017** and the Provider details that as "per [it's] standard process" following the application being received by it "*the applicant is issued with paperwork for signing and for return. This paperwork was issued on **12 May 2017**, addressed to the Complainant and dispatched to his correct correspondence address* [Irish address redacted]".

The Provider submits that the "account opening paperwork was signed and dated **25 May 2017"** and was received by the Provider on **30 May 2017**.

The Complainant's debit card for this account was dispatched by the Provider on **8 June 2017**.

In a telephone call to the Provider on **9 June 2017,** the caller states that he is in Switzerland, that he does not have his debit card and needs a replacement card sent to him in Switzerland. He states that he has lost his debit card. He is told he will not be able to get a replacement card sent to Switzerland, and even if it could be sent there it could take 2 weeks. He states that even 2 weeks "could be ok". It is suggested that he uses his other debit card (until he gets home). This suggestion does not appear to be satisfactory to the caller. He remains keen for the Provider to send a new card to him at a Swiss address. He receives confirmation that the Provider will not send a replacement card to Switzerland, but is offered the option to cancel the card and have a replacement sent to the address in Dublin that the Provider holds for him, or for it to be sent to a branch of the Provider. He declines these offers. He asks for it to be "issued" to the branch closer to where his Dublin address is. He is told that for this to happen he will have to be transferred to the lost and stolen credit card department. The caller's line cuts off before the he gets to speak to this department – apparently whilst the Provider's agent is explaining to another agent that the caller wishes to cancel his card and arrange a replacement.

At no point during this call is the Complainant's card cancelled, nor is a replacement issued. However, it appears that some form of restriction was placed on the card as a precautionary measure. This is evident from the next phone call.

I accept that if the Provider were to have acceded to a request to send a new debit card to any address other than an address in the state confirmed by the Complainant to be one at which he was resident that would have given rise to obvious security concerns. In this context, I would point to Section 12.3 of the account terms and conditions which provides that *"If your name, address, telephone number or email address changes, you must tell us immediately..."*

/Cont'd…

The Complainant had at least 3 different addresses on file (two in Ireland and one in Australia) during the period 2016-2018. No explanation has ever been put forward as to what may have happened to mail sent to a particular Irish address, and even now it is not clear whether, or for how long, the Complainant was actually living at that address when he gave it to the Provider when opening the account on 25 May 2017. The Provider raises an issue in this regard and it is dealt with later in this decision.

The Provider has given an explanation (and furnished an audit trail) which clearly shows that transactions were carried out on the online banking platform. The Complainant's online banking password was reset on **14 June 2017**. The Provider has explained that, where a customer cannot remember their PIN or Password, on input the correct full name and date of birth, an activation code is sent to the customer's registered telephone number.

The Complainant states that he received no such text. However, the Provider has advised that on that date, there is no record of an activation code being sought, meaning that the correct PIN and Password was entered.

The Provider has stated that the forgotten PIN/Password procedure (SMS to the Complainant's mobile number to change PIN/Password) was previously carried out on 11 May 2017, and there appears to be no issue taken in the sense that the procedure was successfully utilised by the Complainant on that occasion.

On **15 June 2017** a caller telephones the Provider. This appears to be a different person to the person who called on 9 June 2017. He provides the Complainant's full name and the correct card number (which would not be particularly difficult for anyone who is in possession of the card). This caller is then asked for his birth month and year and the first line of his address, both of which he answers correctly. He correctly answers what branch the account is held with, and that he has no direct debits or standing orders. He also correctly answers that a payment was made into the account “from my other account” within the past hour or so. He is asked what age he will be on his next birthday (which can be divined from the answer to the earlier birth month/year question in any event). He states that he attempted a transaction in a casino which was declined, and another in a pub which was declined.

The restrictions are lifted on the basis that all security questions have been answered and the card is ready to be used again. Over the next week or so the card is used to carry out numerous transactions which are disputed by the Complainant.

The Complainant has furnished extensive receipts to this office to show that he was in the UK on 13 – 17 June 2017; in Poland on 18 – 29 June 2017; and, in Vienna on 1 July 2017. In reality, the only thing that this documentation definitively proves is that transactions were carried out in these places during these dates using debit cards other than the card ending 7799. During this time (mid to late June), statements show that the card ending 7799 was being used in Dublin.

/Cont’d…

On **30 June 2017** what appears to be the same caller as the 9 June 2017 calls the Provider. He states that his card has not been lost or stolen but that he is in Austria and his card is not working to pay for his hotel. The caller is told that the telephone agent is unable to access his details, but a letter has been sent to him explaining the issue.

It is now known that this was due to the fact the accounts had been closed by the Provider. The Complainant is understandably frustrated. This is exacerbated by the fact that the Complainant is away from his address.

The Complainant telephones the Provider again on **3 July 2017**. Unfortunately, the same impasse is reached whereby the Provider's agent is not able to assist any further.

I note at this point that it would not be reasonable to expect that any agent of a provider would recognise the voice of a caller on any given call. This is the reason security questions are of such central importance.

It was the access to the online banking platform from (at the latest) 14 June 2017 onwards that gave rise to all of the problems that followed.

Payment Services Regulations and "Gross Negligence"

I am satisfied, and the Provider accepts, that these transactions were subject to the provisions of the **European Communities (Payment Services) Regulations 2009** ("the Regulations"). The transactions occurred during June 2017 and therefore predate the European Communities (Payment Services) Regulations 2018.

The Complainant is a payment service user and the Provider is a payment service provider within the meaning of the Regulations.

Regulation 70 places an obligation on a payment service user to notify the payment service provider of the theft, loss or misappropriation of the payment instrument or its unauthorised use without undue delay, and further provides that:

> *"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"*.

The Provider contends that the Complainant did not take such reasonable steps and accordingly did not comply with his obligation to do so under Regulation 70.

/Cont'd…

Regulation 72:

> *"A payment service user is entitled to rectification from a payment service provider of an unauthorised or incorrectly executed payment transaction giving rise to a claim (including a claim referred to in Regulation 90) only if he or she notifies the payment service provider without undue delay on becoming aware of the transaction...."*

Regulation 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 services 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 or her obligations under Regulation 70."*

Regulation 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 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 details 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".*

It is clear from the wording of Regulation 75 that differing degrees of responsibility upon cardholders are envisaged in relation to losses incurred through a failure to keep their security features safe. A customer can be required to bear a loss up to €75 if the security details have been lost or stolen (or up to €63.49 if the card is lost/stolen).

Section 9 of the terms and conditions for the Complainant's current account mirror the above regulations but use the term "gross lack of reasonable care" rather than "gross negligence". For the purposes of this complaint, I do not consider "lack of reasonable care" to be different to, or distinguishable from, "negligence".

The Provider contends that the Complainant must have made the payment himself or must have acted with gross negligence.

The term "gross negligence" is not defined in the 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 by both the High Court and the Supreme Court in the case of ICDL Saudi Arabia v European Computer Driving Licence Foundation [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"*.

The Provider has made a number of post Preliminary Decision submissions. These included comments regarding the security of their own system. The Provider also repeated its belief that the volume of personal information used should be considered by me. In that regard I would point out that all evidence and submissions have been considered by me in arriving at my decision.

/Cont'd…

In its post Preliminary Decision submission, the Provider states:

> *"Bearing in mind there was no evidence to suggest the Complainant was the victim of vishing or phishing, if we examine the amount, and nature, of personal security information pertaining to the Complainant's account required to carry out all the disputed transactions our view is that the only way a fraudster could have obtained each individual piece of information (in the absence of fraud or intentional failure on the Complainant's part per Regulation 93) is for there to have been "a significant degree of carelessness" on the Complainant's part in safeguarding all of his personal security information (including the Anytime PIN and Anytime Password he generated himself) thereby enabling them to be obtained and used by someone else (i.e. gross negligence per Regulation 98(3)(b)). This would be a breach of the Regulations and our Personal Banking Terms and Conditions, a copy of which has previously been furnished to your office.*
>
> *Again we stress that it is not just a card PIN or a card number at issue here, it's practically every unique item of personal security information the Complainant has, some of which wasn't bank generated and which only the Complainant knew having had to generate it himself".*

It also submits:

> *"If it is in fact the case that the Complainant wasn't in Ireland during the account opening period he would have been well aware the account opening paperwork and the Debit ServiceCard would have been sent to his address in Balbriggan while he was out of the country. We would be interested to hear his explanation in relation to the completion and return of the account opening paperwork to us while he appears to have been in Europe.*
>
> *On the basis that he appears to have been in Europe when the account was opened and the Debit ServiceCard was issued to his address in* [Irish address]*, it would seem to us that his call to us on the 9 June 2017 to say he couldn't find his card was disingenuous in circumstances where he knowingly could never possibly have been in physical receipt of the card in the first place, due to the fact it having been sent to his address in [Irish address] while he was abroad.*
>
> *Accordingly, the question which remains to be answered is how the Complainant could have been in Dublin opening an account which was immediately thereafter the subject of disputed transactions, and simultaneously been in mainland Europe using his other [the Provider's] Debit* Card? We submit that this goes to the heart of the credibility of the Complainant's position for the entire complaint".

/Cont'd…

The Provider further submits that it has:

> *"also now provided cogent evidence in terms of specific transactions occurring on account [*****045] which appear to indicate the Complainant allowed someone else complete the account opening of account [******588] on his behalf while he was abroad. It has to now be considered that if this is what happened what other personal/security information did the Complainant allow or enable someone else access to either knowingly or through a "significant degree of carelessness".*
>
> *When taking into consideration the manner in which account [******588] was opened at the Complainant's request whilst he appears to have been out of the country and noting that all relevant account opening documents (which were accessed, completed and returned) were sent to the same address which the associated debit card and PIN were subsequently sent to, our position is that there are too many coincidences at play to discount the very strong likelihood of "a significant degree of carelessness", too many coincidences to discount the very strong likelihood of gross negligence on the Complainant's part".*

In its conclusion to its post Preliminary Decision submission dated **11 December 2020**, the Provider details that:

> *"In light of the above submissions we would raise serious concerns around the manner in which the Complainant opened this account, his location (pre and post account opening), his candour and his intentions. We believe we have evidenced that there has been a significant degree of carelessness on the Complainant's part and we would be obliged if you would reconsider your Preliminary Decision and reverse the direction that we pay compensation and refund the disputed transactions which total €11,032.08"*

The Complainant, in a post Preliminary Decision submission, responded:

> *"This statement from* [the Provider] *is complete and utter nonsense. Maybe instead of playing this victim blaming game and saying their systems are amazing and not believing a word I say they should review the facts and see that their security protocols are completely laughable and improve them for the future as it is a fact they are inadequate when a fraudster can contact* [the Provider's] *fraud department and with complete ease unblock an account like they did with no real security questions in the recorded voice call provided in evidence".*

The Provider made a further post Preliminary Decision submission in response the Complainant's submission in which it states:

> "*The Complainant has not provided any explanation, clarity or evidence to dispute the points made in our communication of 11 December 2020 relating to:*

/Cont'd…

Circumstances Surrounding the Opening of Account Number 11055588: *We raised the point that the Complainant has never disputed the fact that account number [*******588] was opened in his name. Nor has he ever disputed the fact that a Debit ServiceCard was ordered and dispatched on this account, despite fact that it is now clear that these were being arranged for him, in good faith by the Bank, at a time when he was not physically in Ireland. The Complainant has failed to respond to this point.*

Account Opening Timeline Vs Complainant's Travel Timeline: *The above numbered account and associated Debit ServiceCard (ending 7799) were being opened and arranged for the Complainant even though the records on the Complainant's Standard Account [******7045] show that he was in mainland Europe during May 2017 when he requested the second current account [******588] to be opened. Based on the Complainant's own submissions, he remained out of Ireland during the course of June and July 2017. We stated that we would be interested to hear his explanation in relation to the completion and return of the account opening paperwork to us while he appears to have been in Europe. The Complainant has failed to respond to this point".*

The Provider further states:

*"In light of the points made in our letter of 11 December 2020, we stated that we would be interested to know on what date the Complainant departed Ireland, particularly in light of the fact that his account statement for [*******7045] shows that there were a number of card transactions carried out across Europe during the months April, May and June 2017. However, the Complainant has not provided any response to this query in his email of 14 December 2020.*

Despite the opportunity which we have given for the Complainant to clarify the above matters, rather than address these points, he has instead decided to focus on points which he had previously raised during the course of the complaint Investigation with your Office, and to which the Bank had previously provided its comprehensive responses".

Analysis

I am not satisfied there can be any real dispute on the application of Regulations 70 and 72 insofar as the notification is concerned – there is no evidence of undue delay on the part of the Complainant in notifying the Provider of these disputed transactions.

He did so on July 3. I do not believe a failure to check online banking details daily or more regularly over the previous couple of weeks constitutes sufficient grounds for coming to a different view. Even where the online banking platform had been accessed during June, it cannot be known whether these logins were by the Complainant himself or by a third party who was in possession of all of his details.

/Cont'd…

There is no evidence that the Provider's systems failed or were somehow bypassed. The circumstances of this complaint make it clear that access to the online banking platform was the crucial element that allowed these transactions to take place. The audit trails provided show that the correct PIN and password were used to log in to the online banking platform.

I am not satisfied there is any evidence that the Provider's own systems caused or contributed to these transactions being carried out.

Criminal activity is a matter for the Gardaí and the Courts and as such is outside the remit of this Office in line with **Section 52(d)** of the **Financial Services & Pensions Ombudsman Act, 2017**. The Provider is under a duty to cooperate with any such investigation. There is no evidence that the Provider has failed in that duty.

Once the Provider makes a decision to terminate the bank/customer contract, it is entitled to do so in accordance with the terms of the account. Section 5.1 of the current account terms (cited in the notice of account closure letter dated 26 June 2017) states:

> *"Unless the additional Terms and Conditions in Sections C and D provide otherwise, this Agreement has no minimum terms and will continue until terminated by either You or us in accordance with this Agreement.*
>
> *Your Account will remain open until it is closed by either You or us in accordance with this Agreement".*

It does not seem that Sections C or D described above have any material impact on this section. Section 5.2 states that notice periods of 60 days or 30 days will be given for closures in respect of payment accounts or non-payment accounts, respectively.

I can find no authority for the proposition contained in the Notice of Account Closure letter that the account terms permitted the Provider to close the Complainant's account(s) *"within 7 days".*

In relation to the debit card and PIN, these were sent to the Complainant's address but he was not there. It is my view that, in and of itself, being away from your address while a card and PIN is sent in the post does not constitute gross negligence but does fall within the ambit of Regulation 75(1) where the cardholder is liable to bear a loss up to €75 in total.

The crux of this complaint is whether or not the Provider has wrongly concluded that the Complainant acted fraudulently or intentionally or failed, because he acted with gross negligence, to fulfil his obligation to keep his online banking PIN and password safe.

The simple fact that the correct online banking PIN and password was used is not in and of itself necessarily sufficient evidence for the Provider to rely on.

/Cont'd…

In addition to many security questions which a third party could find an answer to by, for example, having access to an abundance of personal mail, social media accounts, and/or identification documentation, this caller was also in a position to describe transactions made in the previous hours through the online banking platform. The Provider asked numerous questions to which the caller had all of the correct answers. The third party was in possession of every piece of security information that could be reasonably required.

The home address issue is relied upon by the Provider as evidence of gross negligence, over and above the mere fact that the correct online PIN and password were used. In its submissions it states that the Complainant *"provided an address in [Ireland], which he later advised the Bank he was not living at. Therefore, unknown to the Bank when ordering the Card for the Complainant, this was not possibly a secure address for delivery of the Card and PIN which were subsequently used for the online transactions, Point of Sale Transactions, and Cash Withdrawals"*.

Furthermore, the Provider describes the Complainant's initial statement during the phone call of 9 June 2017 that the card was "lost" as being *"vague and unqualified"*. It contends that, although the Complainant initially states that his card was "lost", he could not have received it by that stage as he was already in Switzerland, and the card was only dispatched to his Dublin address on 8 June 2017.

The Provider also repeats that the only possible explanations for the correct online PIN and password being used are either that the Complainant carried out the transactions himself, or acted with gross negligence in failing to keep those details safe.

The reason the Complainant's account security was apparently compromised was, ultimately, because a third party came into possession of extensive personal and security information; his debit card; cheques made out to him; and – most crucially – his online banking PIN and Password, such that this third party was in a position to effect online transfers and use a debit card.

In attempting to put forward evidence of "gross negligence" (and in addition to the mere fact of the extent of information that appears to have fallen into the hands of a third party) the Provider points to ambiguity surrounding the Complainant's address, and whether or not the address he gave when opening his account on 25 May 2017 was a permanent address and/or one at which he would safely receive mail (when he was travelling for most of June). It also contends that he could not have "lost" his card by 9 June 2017 when he was in Switzerland, as the card would not have arrived to his Dublin address by then.

The Provider has detailed that the Complainant ordered the new card while he was out of the jurisdiction and that it appears he was still away when the paperwork was completed and submitted. I am not entirely sure what the Provider is asserting in this regard. If it is the case that it believes that there was a possible fraud, then I would expect it would have notified the matter to the Gardaí.

/Cont'd…

I note the Provider has questioned the Complainant's candour and his intentions. Its position is that *"there are too many coincidences at play to discount the very strong likelihood of "a significant degree of carelessness", too many coincidences to discount the very strong likelihood of gross negligence on the Complainant's part."*

The Provider appears to miss the requirement for it to produce evidence and not to simply attempt to question the character of the Complainant and rely on likelihoods, whether strong on not.

I remain of the view that the matters put forward by the Provider, both in its original submissions and its post Preliminary Decision submissions are, ultimately, conjecture and not evidence. Furthermore, they do not appear to relate in any way to the online PIN and password, which were the final, and crucial, keys used to unlock the Complainant's accounts for the disputed transactions.

On balance, I remain of the view that the Provider has failed to produce sufficient evidence to conclude that the Complainant acted intentionally or fraudulently or failed to fulfil his obligations under Regulation 70 by reason of gross negligence. 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).

The lodging of cheques is a matter which can be done by a person other than an accountholder. The cheques were lodged to accounts of the named payee. Not only does no security issue arise with this practice in and of itself, but it also results in a convenience that would be lost if the accountholder had to make the lodgement him/herself in all circumstances.

Accordingly, I direct the Provider to refund the total amount of the disputed transactions (less the sum of €75 for which he is liable pursuant to the account terms and conditions).

Finally, a provider is entitled to end the banking relationship without providing a reason. In this case, it is unfortunate that the Complainant was not able to receive the notification letter as he was away on holidays. This is not the fault of the Provider.

However, I can find no authority for the proposition that the Provider was entitled to close the account(s) on 7 days' notice. This short notice period, admittedly exacerbated by the fact the Complainant was abroad, gave rise to an even more difficult set of circumstances for the Complainant to contend with. I fully appreciate that the swift closure of the account may well have prevented further frauds from being perpetrated, however the Provider has not sought to make this point and, in any event, the same outcome could have been achieved by putting a freeze on the account.

For the reasons set out in this Decision, I substantially uphold this complaint and direct that the Provider pay the value of the disputed transactions (€10,607.08), less €75.00, plus €500 by way of compensation (for a total of **€11,032.08).**

/Cont'd…

Conclusion

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

Pursuant to ***Section 60(4) and Section 60 (6)*** of the ***Financial Services and Pensions Ombudsman Act 2017,*** I direct the Respondent Provider to pay the value of the disputed transactions (€10,607.08), less €75.00, plus €500 by way of compensation (for a total of **€11,032.08)** to the Complainant. This sum is to be paid 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

6 December 2021

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,

/Cont'd…

(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.