An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

Decision Ref:	2021-0008
Sector:	Banking
Product / Service:	ATM
Conduct(s) complained of:	Failure to provide adequate security measures Handling of fraudulent transactions
Outcome:	Upheld

LEGALLY BINDING DECISION
OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

This complaint relates to unauthorised transactions on the Complainant's account and the Provider's refusal to indemnify the Complainant for the losses incurred arising out of these unauthorised transactions.

The Complainant's Case

The Complainant holds a current account and a related Visa Debit card with the Provider. Between **12 and 16 February 2018**, 13 transactions were processed from his account which the Complainant states were not authorised by him. In relation to the 13 transactions, 6 were ATM withdrawals totalling €1,500, 4 were point of sale transactions totalling €1,750.94 and 3 were internet transactions totalling €17,230. In total, the Complainant states that he has suffered a loss of €20,480.94. On **13 February 2018**, the Provider flagged the point of sale (POS) transactions as suspicious and contacted the Complainant to investigate if the Complainant had authorised the transactions. The Complainant told the Provider he had not. The Complainant states that he only discovered the true extent of his losses on **16 February 2018**. He further states that it transpired that the Provider had issued a replacement debit card without his request and that he had never received it and that this was the card used to effect the fraudulent transactions.

The Provider declined to refund the monies taken from the Complainant's account on the basis that he was still in possession of his debit card, there had been no recorded PIN errors, no point of compromise for the PIN and no sign of third party fraud, vishing or phishing scam.

The Complainant disputes the Provider's findings of fact and its decision not to refund the monies.

The complaint is that the Provider failed to exercise reasonable care and skill in its dealings with the Complainant and in particular has wrongfully, unreasonably and through a mistake of law or fact refused to indemnify the Complainant for the loss in question. The Complainant is seeking a refund of all the monies taken from the account as a result of the fraud.

The Provider's Case

The Provider has stated that it will not refund the losses incurred because it disputes whether the transactions were unauthorised and if they were, then given the security measures put in place by the Provider, it states that the Complainant must have allowed a third party access to this security information and in doing so, he failed to comply with his framework agreement and by doing so he breached the European Communities (Payment Services) Regulations 2018. The Provider asserts the Complainant's actions amounted to gross negligence within the meaning of the European Communities (Payment Services) Regulations 2018.

The Provider submits that the replacement debit card was requested through the Complainant's online banking account, and it was issued to the Complainant's registered address. The Provider states that while the Complainant disputes ordering this card, it states that no new PIN was issued with the card and therefore questions how a third party came into possession of the correct PIN to enact the fraudulent transactions.

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.

/Cont'd…

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 27 April 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 Provider to this Office dated 20 May 2020.

2. E-mail, together with attachments, from the Complainant to this Office dated 26 May 2020.

3. E-mail from the Provider to this Office dated 12 June 2020.

4. E-mail, together with attachments, from the Complainant to this Office dated 16 June 2020.

Copies of the above submissions were exchanged between the parties.

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

At the outset, I must point out that I am satisfied that the European Communities (Payment Services) Regulations 2018 are applicable to this complaint. I note the Provider has accepted in its submission to this Office that the transactions carried out were subject to the provisions of the European Communities (Payment Services) Regulations 2018 (the "2018 Regulations"). The 2018 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 by means of a Payment Instrument (that is, physical devices [such as cards] and/or [a] set of procedures).

The Complainant denies that he authorised any of the disputed transactions. The Provider disputes that the transactions were unauthorised or, if they were, then it asserts that the only other explanation is that the Complainant enabled his personal banking information including his visa debit PIN number, Anytime Banking PIN number and [online] Banking password to be shared with another party who was not authorised to have such information.

/Cont'd…

As mentioned above, in this case, between **12 and 16 February 2018**, 13 transactions were processed from the Complainant's account which the Complainant states were not authorised by him. It is relevant to distinguish that in relation to the 13 transactions, 10 were carried out by use of a visa debit card and PIN (6 ATM withdrawals totalling €1,500 and 4 POS transactions totalling €1,750.94) and 3 were internet Banking transactions totalling €17,230.

The following details of the disputed transactions were furnished by the Provider in its response to this Office:

12 February 2018	€200	13:12.13pm	Convenience store, Dublin 8
12 February 2018	€200	13:12.49pm	Convenience store, Dublin 8
12 February 2018	€200	13:13.38pm	Convenience store, Dublin 8
12 February 2018	€150	13:14.20pm	Convenience store, Dublin 8
12 February 2018	€13,000	13:28pm	online transfer to another a/c
12 February 2018	€3,000	12:57pm	online transfer to another a/c
13 February 2018	€600	12:34.39pm	ATM, Dublin 1
13 February 2018	€150	12:35.24pm	ATM, Dublin 1
13 February 2018	€22	12:36.51pm	Convenience store, Dublin 1
13 February 2018	€638.20	12:58.23pm	An Post Office, Dublin
13 February 2018	€487.35	13:15.04pm	An Post Office, Dublin
13 February 2018	€603.39	16:25.43pm	An Post Office, Dublin
14 February 2018	€1,230	22:06pm	online transfer to another a/c

Having reviewed the documentation provided in evidence, I accept that in relation to the 10 visa debit transactions, they were carried out using CHIP card, that the card was present and that the PIN was entered and verified. In relation to the 3 internet Banking transactions, I am satisfied that they were executed by navigating successfully each of the security steps put in place by the Provider.

In total, the Complainant states that he has suffered a loss of €20,480.94. This figure is borne out by the transactions listed above. On **13 February 2018**, the Provider flagged the POS transactions as suspicious and contacted the Complainant to investigate if the Complainant had authorised the transactions. The Complainant told the Provider he had not. The Complainant states that he discovered the true extent of his losses on **16 February 2018**. He further states that it transpired that the Provider had issued a replacement debit card without his request and that he had never received it and that this was the card used to effect the fraudulent transactions.

The three internet transactions in the amounts of €13,000, €3,000, and €1,230 respectively were transferred online to the same third-party account. The Provider submits that in light of the fact that the Complainant disputes the carrying out of these transactions, it is relevant to set out the process and security steps required to be undertaken before these types of payments can be carried out online.

/Cont'd…

The Provider goes on to explain that in order to log on to an [online account], the customer must first enter either the customer number or their card number. Once this has been done, the customer is brought to the next screen in which they are asked to enter both their [online account] PIN number and their [online account] password.

In addition to all of the above, the Provider makes the point that as these were new third party payments, the customer is required to insert his Visa debit card into a card reader issued by the Provider to its online banking customers. When prompted on the card reader, the customer must then input the PIN number that applies to the Visa debit card in question into the card reader. This generates a transaction code on the card reader which the customer then has to input into the relevant field on [online account].

The Provider explains that it is only when this authorisation process is followed, that a customer will be able to complete an online banking transaction to a third party account. I am satisfied that this is an accurate description of the process that would have had to have been followed in order to execute the three disputed internet banking transactions.

It appears from the submissions of both parties and the documents furnished to this Office that the disputed transactions emanate from a replacement Visa debit card that was ordered on the Complainant's account on **5 February 2017**. The Provider, upon receiving this request, which the Complainant states he did not make, issued a new Visa debit card (ending 3217) to the Complainant's registered correspondence address. It is this card, ending in 3217, that was used to carry out the 10 disputed Visa debit card transactions. It is unclear, whether this card was used to get past the first described step of logging in to [online account] but it does appear, on balance, that this card, ending in 3217, may have been central to all of the disputed transactions given the proximity between the dates when the card was issued and the execution of the disputed transactions.

The Complainant denies having ordered the new Visa debit card and in addition, he denies ever having received it.

In my Preliminary Decision I cited Regulation 96 (3) of the 2018 Regulations which provides:

> *(3) Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, including a payment initiation service provider as appropriate, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Regulation 93.*

In light of the foregoing provision and in the circumstances of this case, I indicated my acceptance that the disputed transactions were unauthorised for the purposes of the 2018 Regulations.

There have been significant post Preliminary Decisions submissions in which the Provider has argued that I erred in law, and that it has provided additional points of fact, which it believes should alter my decision.

/Cont'd…

The Provider has, in its post preliminary submission dated **19 May 2020**, detailed the timeframe regarding the disputed ordering of the replacement card.

The Provider states:

> "*The replacement debit card was ordered through the Complainant's* [Online banking] *account on Monday 5th February 2018 and dispatched Wednesday 7th February 2018. When a replacement card is ordered online the message the user sees is that they will receive it within 5 working days. Our cards are dispatched from one of our centers in* [different jurisdiction] *by standard* [named postal service]. *Per the* [postal service's] *website, it has an estimated delivery time for 'standard' mail to Europe of 3 to 5 days.*
>
> *In a best case scenario, the replacement card could potentially have arrived between Thursday 8th February 2018 or Monday 12th February 2018. The first disputed transaction occurred on the 12th February 2018."*

The Provider further details that:

> *"The Complainant lives in the* [named apartment complex] *development in Dublin* [post code] *and we have enclosed images from Google maps which show what appears to be security coded/ locked gates into the development. Furthermore, we enclose a photo from an online auctioneer's listing depicting the interior ground floor hallway image for the apartment building matching the Complainant's address. You will note from same there is an external security coded/ locked door into the lobby and individual mailboxes for residents which in the ordinary course are secured by keys held by the respective occupants".*

The Provider then puts forward the argument that:

> *"for someone to successfully have intercepted the item of mail containing the replacement debit card they would have had to gain access to the apartment building via the security doors and finally gain access to the locked mailbox on the exact date on which the card was delivered not to mention accounting for the time of day post is delivered- if they arrived too early they'd have had to wait or come back. If they arrived on the wrong day they'd have had to leave and come back the following day. In essence someone would have had to stalk the mail box, and gain access to it, until they got hold of the letter.*
>
> *Our view is that this sequence of events to intercept the item of mail from the Complainant's mailbox does not stand up to scrutiny. We would pose the question; would a more plausible explanation be that someone living within the apartment building gained access to the Complainant's mailbox?"*

/Cont'd…

The Provide also highlights that:

> *"all of the disputed ATM and Point of Sale transactions were carried out within a 2.5K walking distance of the Complainant's address. We would further add that it is also worth noting that the holding Bank for the beneficiary account for the disputed transfers was less than a 1k walking distance from the Complainant's address."*

The Complainant responded to the above statements, in his post Preliminary Decision submission dated **26 May 2020** as follows:

> *"First, I never ordered the debit card from the provider.*
>
> *Second, if the provider sent the Debit card to my home address as they claimed, the building is not as secured as the provider stated, the security Code/Locked (sic) for the gate and the security Code/Locked for the front door of the building never worked since I moved in the* [named apartment complex], *There is one single key for the gate and the front door of the building, also inside the housing estate there are another three buildings next to each other operating by the same single key. So, there are four buildings and front gate operating by one single key, in this housing estate there are more than three hundred apartments, so you can imagine the traffic and how many people has access to those buildings. However, all of that if the provider truly sent the Debit card to my home address.*
>
> *About the short distance of the transactions of my home address also this a poor excuse from the provider, short distance of the transactions of my home address doesn't mean I was neglect, I live in* [named location in Dublin]*, it's about 15 mins walk from the heart of city centre where most of major business, shops and banks are. I believe it's the ideal spot for the fraudulent to make the transactions. This is my point of view and hope this make sense to the provider."*

The Provider responded to the Complainant's comments in its second post Preliminary Decision submission dated **12 June 2020.**

The Provider states that:

> *"the replacement debit card was issued to the address on file*, [address given]. *We note the Complainant's statements regarding the security arrangements in his apartment complex and that four separate apartment buildings (and the front security gate) use the exact same security key. Notwithstanding this however, it still doesn't account for the interception from the Complainant's secured mailbox. Again we pose the question, would a more plausible explanation be that someone living within the apartment building gained access to the Complainant's mailbox?"*

/Cont'd…

The Provider further states that:

> *"Our point in relation to the proximity of the disputed transactions and the location of the holding Bank for the beneficiary account for the disputed online transfers is that it arguably points to the transactions having been carried out by someone in the same locality as the Complainant which ties in with the point we have made in relation to the interception of post from the Complainant's secured mailbox".*

While the submissions of the Provider show the front security gates to the apartments, and indeed a row of secured mailboxes (some are ajar), the photos also show that some mail has been left on the top of the mailboxes.

I do not believe that the Provider's arguments regarding the proximity of the disputed transactions are convincing. The Complainant is resident in a very central location, and I do not accept that as the transactions occurred within close proximity to his residence that this in some way evidences that he was at fault for the fraudulent transactions or 'careless' with his personal details.

I also note the Provider's suggestion that this indicates that the transactions were carried out "*by someone in the same locality as the Complainant*" or that *"someone living within the apartment building gained access to the Complainant's mailbox*". I accept that either or both of these scenarios are entirely possible, particularly given that the development concerned incudes hundreds of apartments in a heavily populated, busy area of Dublin. If the Provider is correct in these suggestions, as it well may be, I fail to see how it advances its position.

In its post Preliminary Decision submission, the Provider submits that the actions of the Complainant after its call to its fraud department, should be considered an additional point of fact.

The Provider states that:

> *"In the Complainant's letter to your Offices dated 15/02/19 [sic] he references his call with our fraud team at approximately 18.26pm on the 13th February 2018…and how after learning that his account had practically the entire balance debited he went to check his account online a little later after the call. He made the following statement, 'later on, on the same day 13/02/19 [sic] I went home and I tried to login into my internet banking just to check and the system didn't allow me to login'".*

The Provider details that its:

> *"…records indicate no failed login attempts on the 13th February 2018, conversely what they do evidence is a successful login at 19.44pm and successful statement enquiry at 19.45pm".*

/Cont'd…

The Provider continues its submission and states what it believes is the next logical action a person would take after a call to its fraud department is to try log in and view a balance statement. The Provider also states that from viewing its submission of the Complainant's online history:

> *"it confirms the IP address used for the login as [XXX.XX.XX.XX.] that is precisely the same IP address that was used to carry out the disputed online transaction at 12.56pm earlier on the 13th February 2018."*

The Provider states:

> *"if the Complainant did actually check his account balance at 19.45pm on the 13th February 2018 …then it would appear that the login originated from the same IP address as that which was used to access the online account to conduct the disputed transaction from earlier that same day. As the Complainant denies carrying out the earlier transaction, the question we would ask is who else might be in a position to gain access to the Complainant's device(s)?"*

The Complainant responded to the Provider's comments regarding his log in activity in his post Preliminary Decision submission dated **26 May 2020**, while also highlighting that the Provider failed to block his account after he reported the suspected fraud:

> *"On the 13th February 2018 I did try to log in to my internet banking late that night but I didn't succeed, I tried only once and I didn't insist presuming my bank card and my internet banking were blocked by the provider, even the provider on that call said in order for me to get access to my bank account, I have to go to my branch with my ID.*
>
> *For me what's normal, logic responds/ action to take in these circumstances is **not to log in** to my internet banking as its supposed to be blocked by the provider straightaway after that call at 18:30 and no one supposed to have access to it. The provider fails to do so and blocked only the Debit card that I had in my position and left the second Debit card that they issued few days ago active, the same debit card that the fraudulent used and neither I or the provider were aware of the existence of this card at that time. Also left internet banking open even I denied I made any online transactions on that day resulting the loss of the rest of fund from my bank account on 14th February 2018".* (Complainant's emphasis added)

The Provider, in its post Preliminary Decision submission dated **12 June 2020**, acknowledged its error in not having blocked the Complainant's account following the reporting of the potential fraud to its fraud department, and makes an offer of compensation to the Complainant for this:

> *"Having reviewed this aspect of the online account remaining open after the Complainant's call with us on the 13th February 2018, in retrospect, we consider this to be an error on our part and we sincerely apologise.*

/Cont'd…

> *Accordingly, we are satisfied to reimburse the Complainant in respect of the final disputed transaction (online transfer in the sum of €1,230.00) which occurred on the account on the 14th of February 2018. In acknowledgement of this customer service failing we would also like to make a goodwill gesture of €1,000.00 to the Complainant".*

The Complainant, in his post Preliminary Decision submission dated **16 June 2020**, submits that:

> *"I don't take the €1000 offer from the provider as a goodwill gesture but as an* [admittance] *from the provider they are in a wrong. It's a shameful offer that I proudly decline, I don't accept less than what the provider lost from my account with them less €50 as per rules, also a compensation of more than two years of stress and time wasting from the provider".*

It is surprising that the Provider does not appear to have noticed this significant error as part of its original investigation of the matter.

The Provider has commented on the log in details and the IP address relating to certain occasions when the account was accessed. This is of limited value in terms of identifying who was accessing the account, particularly when furnished for a limited use and period of access to the account.

The Provider has, in its post Preliminary Decision submission dated **19 May 2020**, put forward the argument that I made an error of law when I stated:

> *"The Provider has been unable to provide this Office with any evidence that supports gross negligence on the part of the Complainant".*

The Provider submits that:

> *"The Regulations are silent as to the definition of 'gross negligence' however, in a 2012 Irish case, ICDL GCC Foundation FZ-LLC & Anor v European Computer Driving Licence Foundation Ltd [2011] IEHC 343, the High Court addressed the concept of 'gross negligence' in a commercial contract and held the defendant acted with a significant degree of carelessness such as to amount to gross negligence".*

The Provider highlights that:

> *"On appeal to the Supreme Court in 2012 the decision was upheld with the Supreme Court agreeing that the concept of gross negligence involved 'a significant degree of carelessness'. This appears to be the current jurisprudence on the definition of 'gross negligence' in Ireland".*

/Cont'd…

The Provider further argues that there is no evidence that the Complainant:

> *"was the victim of vishing or phishing" and "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 thereby enabling them to be obtained and used by someone else (i.e. gross negligence per Regulation 98(3)(b))"*
>
> [Provider's emphasis added]

The Provider then details the type of personal data that would have been required and their use. The Provider states that:

> *"In this case practically every individual piece of personal security information pertaining to the Complainant's account has been used…our view is that in the absence of fraud or intentional breach of our terms and conditions by the Complainant then it is just not credible that there wasn't a 'significant degree of carelessness' on his part to safeguard all his personal security information".*

The Provider reiterates that:

> *"It's 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 the Complainant had to generate himself.*
>
> *Our belief 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".*
>
> [Provider's emphasis added]

The Complainant has responded to the Provider's submission in his post Preliminary Decision submission that:

> *"The provider still denies the weakness of their security system to protect their customers of been victims of fraud. I include a small paragraph of Dr Ben Smyth School of Computer Science, University of Birmingham, UK. report showing how someone can get access to a customer's online banking easily with just some customers public details".*

The Provider in response submits that the article in question is dated September 2010 and argues that it is not of relevance and disagrees with the statements in the article.

/Cont'd…

The Provider's post Preliminary Decision submission dated **12 June 2020** states that:

> *"In closing we would state that it's not our role to find out who exactly may have been involved or how exactly they obtained every unique item of personal security information from the Complainant. Our objective is to demonstrate on the balance of probability that the Complainant didn't protect his personal security information to the level he is obliged to under the regulations and our personal banking terms and conditions. In the absence of carelessness how do you account for all of the Complainant's personal security information falling into someone else's hands?*
>
> *We take our customer care responsibilities very seriously in the Bank but in this particular case we believe gross negligence facilitated a third party obtaining the Complainant's personal security information and we are challenging the award being proposed. However, as noted earlier, in recognition of our customer service failing in not blocking the Complainant's online banking account after his call with us on the 13th February 2018 our offer of €2,230.00 (€1,230 + €1,000) by way of reimbursement, goodwill gesture and apology is available for the Complainant".*

Despite the Provider's extensive submissions, it remains the situation that it has not produced any conclusive evidence that the Complainant has shown a 'significant degree of carelessness'. Rather it argues that there is a *"very strong likelihood of 'a significant degree of carelessness'"*.

What this Office has to consider is whether the transactions are transactions which the Provider is entitled to refuse to refund to the Complainant pursuant to any of the grounds set out in the 2018 regulations which entitle the Provider to refuse a refund.

Regulation 97 deals with *"Payment service provider's liability for unauthorised payment transactions"* as follows:-

> *97.(1) Notwithstanding Regulation 95 and subject to paragraph (2), where a payment transaction is not authorised, the payer's payment service provider shall—*
>
> > *(a) refund the payer the amount of the unauthorised payment transaction immediately, and in any event not later than the end of the business day immediately following the date that the payer's payment service provider notes or is notified of the transaction, except where the payer's payment service provider has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing,*
> >
> > *(b) where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place, and*
> >
> > *(c) ensure that the credit value date for the payer's payment account shall be no later than the date the amount was debited.*

/Cont'd…

Regulation 98 provides as follows:

> *98. (1) Notwithstanding Regulation 97 and subject to paragraph (3), a payer shall bear the losses relating to any unauthorised payment transactions, up to a maximum of €50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.*
>
> *(2) Paragraph (1) shall not apply where—*
>
> > *(a) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, except where the payer has acted fraudulently, or*
> >
> > *(b) the loss was caused by an act or omission of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced.*
> >
> > *(3) Notwithstanding Regulation 97, a payer shall bear all of the losses relating to an unauthorised payment transaction where the losses were incurred by the payer*
> >
> > > *(a) acting fraudulently, or*
> > >
> > > *(b) failing to comply with its obligations under Regulation 93 either intentionally or as a result of gross negligence on its part.*

Regulation 96 (4) provides:

> *(4) A payment service provider, including, where appropriate, a payment initiation service provider, shall provide supporting evidence to prove fraud or gross negligence on the part of a payment service user.*

This is not one of those cases where there is actual evidence that the Complainant has been subject to a vishing or phishing scam and there is no evidence or *supporting evidence* before this Office that shows or demonstrates that the Complainant has handed over either his card details, his card PIN number, or his [online account] security information pursuant to such a scam or fraud.

It is clear however that in circumstances where the Complainant denies authorising or carrying out these disputed transactions, a third party must have had possession of all of the relevant and necessary security information in order to carry out these disputed transactions.

/Cont'd…

The 2018 regulations state that where a payment transaction is not authorised, the payment service provider shall refund the amount of the unauthorised payment transactions "*immediately*" except where the payer's payment service provider has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing. In this case, there is no allegation that the Complainant has himself engaged fraudulently.

The Provider submits that the Complainant's security information coming in to the possession of a third party *must have been* due to gross negligence and also suggests *the very strong likelihood of 'a significant degree of carelessness'*, such that the Complainant should bear all of the losses incurred as a result of the unauthorised payment transactions.

As outlined above, the 2018 regulations oblige the Provider, in this case, to provide supporting evidence to prove fraud or gross negligence on the part of the Complainant.

In this case, the Provider was asked by this Office whether it believes the transactions were due to gross negligence or fraud of the Complainant in not fulfilling his obligations under Regulation 93 of the 2018 regulations. The Provider has not alleged fraud on the part of the Complainant, but has stated that if the Complainant did not carry out these transactions himself, then the only other explanation is that he allowed or "through negligence" enabled his security information to be shared with another party who is not authorised or entitled to have such information. I note that when asked whether the Provider believes that the Complainant was grossly negligent, the Provider's response was that the Complainant "*must have been negligent*". However, the Provider went on in subsequent questions to contend that the "gross negligence" of the Complainant "*must therefore have been a factor*".

The 2018 Regulations mandate that the Provider must provide "supporting evidence" to establish gross negligence on the part of the Complainant. The Provider's position in this case is that if the Complainant did not carry out the disputed transactions then his security information falling into the hands of a third party must only have been through gross negligence. However, this is not sufficient to displace the burden of proof on the Provider. I cannot make my decision based on an assumption without the Provider furnishing supporting evidence to establish gross negligence. In this case, the Provider has been unable to provide this Office with any evidence that supports gross negligence on the part of the Complainant.

In my Preliminary Decision, I drew attention to the fact the Provider has been unable to furnish this Office with any evidence that supports gross negligence on the part of the Complainant despite the fact that the vast majority of the transactions were carried out through locations and mechanisms that were most likely monitored by CCTV.

The Provider, its post Preliminary Decision submission dated **19 May 2020,** states:

> *"In your preliminary decision of the 27th April 2020 you reference that we provided no evidence of gross negligence 'despite the fact that the vast majority of the transactions were carried out through locations and mechanisms that were most likely monitored by CCTV".*

/Cont'd…

The Provide continues and notes:

> *"Our view is that your Office may have an incorrect understanding of the facts in relation to the bank obtaining 3rd party CCTV footage. No third party retailer would handover CCTV images to us in the absence of a court order. CCTV images would only be made available to An Garda Siochana on provision of a letter signed by a Superintendent".*

The Provider further states that:

> *"it is not our policy to seek 3rd party CCTV when investigating fraud cases and in this instance the Guards have never furnished us with the findings of their investigation (despite our requesting an update) nor have they provided any CCTV footage which they may or may not have acquired".*

The Provider concludes that:

> *"The absence of CCTV footage does not in our opinion undermine our contention that gross negligence has occurred by the Complainant in the safe-guarding of his personal security information further to his obligations under the European Communities (payment services) regulations 2018…and our Personal Banking Terms and Conditions".*

I accept that when the CCTV footage is owned by a third party and not the Provider, it would not be expected to be able to procure this footage.

That said, despite the Provider's extensive post Preliminary Decision submissions, it is still not clear to me what, if any, investigation the Provider undertook into any of the disputed transactions. While the Provider seems to have undertaken further efforts to support its position by undertaking additional research following receipt of my Preliminary Decision, no evidence has been provided to support its position. Neither has any evidence been furnished to show who the beneficiaries of the online transactions were.

I am satisfied that Regulation 98 of the 2018 Regulations applies and which provides that a payer shall bear the losses relating to *any* unauthorised payment transactions, up to a maximum of €50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.

In all of those circumstances, I uphold the complaint and direct that the Provider refund an amount of €20,430.94 to the Complainant (that being €20,480.94 less €50 deducted under Regulation 98). Given that over two years have elapsed since the transactions took place, I further direct the Provider to pay an additional €500 to the Complainant for the inconvenience caused.

/Cont'd…

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) (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 (i) make a compensatory payment to the Complainant in the sum of €20,430.94 and (ii) make a payment of an additional €500 to the Complainant (a total of €20,930.94) 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 payments, at the rate referred to in ***Section 22*** of the ***Courts Act 1981***, if the amounts are 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

18 January 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,

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

/Cont'd…

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