An tOmbudsman Seirbhísí Airgeadais agus Pinsean
Financial Services and Pensions Ombudsman

Decision Ref:	2021-0173
Sector:	Banking
Product / Service:	Current Account
Conduct(s) complained of:	Handling of fraudulent transactions Dissatisfaction with customer service Fees & charges applied Failure to provide adequate security measures Unauthorised withdrawals
Outcome:	Rejected

LEGALLY BINDING DECISION
OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

This complaint relates to disputed transactions on the Complainant's current account held with the Provider between 2014 and 2019.

The Complainant's Case

In a letter of complaint to the Provider dated 23 January 2019, the Complainant submits that he first noticed the disputed transactions in the weeks preceding the letter. He states that he noticed the suspicious activity after reviewing his bank account statement from 2018. He then reviewed further statements and noticed more suspicious activity between 11 February 2013 and December 2018. The Complainant states that the transactions totalled €1,875.63. The Complainant submits that when he became aware of the disputed transactions on the account, he rang the Provider's fraud team, reported the issue and cancelled his debit card.

The Complainant has provided a list of transactions which occurred on his account between 2013 and 2018 as follows:

- EPOCH.com - several payments
- CHG USD - multiple payments

- CHG GBP - multiple payments
- FFN.COM*BOOK - one payment of €20.51
- US currency transactions – multiple payments
- ALC - multiple payments
- GT IDCOSTPRO - multiple payments
- Together NET – 2 payments, €14.90, €29.99
- Tnbillinfo - multiple payments
- Tnwbill.com - multiple payments
- Wmktg*cust-h - one payment of €24.99
- Hubpeople +4 - one payment €34.99
- HP*gowebhel - multiple payments
- FEEREC.COM – multiple payments
- Cscfree.com18 – one payment of €50
- LDpay4aldt.com - multiple payments
- PFA*HONGC SM - multiple payments
- SWEVEB.COM - multiple payments

The Complainant submits that he was unaware of the payments. He states that he was informed by the Provider that it could not investigate suspicious activity on the account more than 13 months old. He requests that the Provider explain how payments were made from his account without his knowledge or authorisation. He argues that small amounts were initially deducted and when they succeeded, larger amounts were taken. He questions how the Provider could authorise the payments without noticing suspicious activity.

The Complainant argues that he was not aware until January 2019 that the payments were being taken out of his account. The Complainant argues that he did not have online banking at the time so was not aware of the transactions and submits that the Provider never informed him of suspicious activity. He states that the Provider has indicated that some of the charges are cross handling charges but states that he was not in America or the UK at the time of the transactions. He states that he is disappointed that this has happened and by the nature of the payments. He states that he was horrified when he googled the transactions to see who was paid and confirms he never used contacted any of the websites in question.

The Complainant wants the Provider to refund the money debited under the disputed transactions.

The Provider's Case

In its final response letter dated 14 February 2019, the Provider states that the transactions for the merchant 'SWEVEB.COM' had been debiting from the Complainant's account since June 2018. It states that its chargebacks department stated that this is a subscription dating service that the Complainant appears to have provided his card details to. It notes that the name appearing on the transactions may be different to the actual merchant name he signed up with.

/Cont'd…

The Provider states that a total of 9 transactions debited from the account from June 2018 and October 2018, however the merchant refunded 7 of these transactions on 5 October 2018. The Provider submits that it would be highly unusual for a merchant to refund an account without contact being made by a customer requesting a refund.

The Provider submits that its chargeback department issued a cancellation request to the merchant in question on behalf of the Complainant on 22 January 2019. It requested that the Complainant contact the Provider without undue delay should he notice any further charges for the merchant in question as the Provider will have chargeback rights in all transactions which may charge after the cancellation request is sent. The Provider states that such disputes are subject to a 120 day timeframe from the date of the transaction.

The Provider refers to the other merchants identified in the Complainant's letter of complaint and states that these are "point of sale" transactions. The Provider states that the merchants all appear to be subscription services that the Complainant entered into an agreement with and provided his 16 digit card details to. It argues that the only way for the Provider to prevent the account being further debited is to issue a request to the merchant bank requesting that they discontinue applying payments to the account. It explains that once a cancellation request is sent to a merchant, the Provider has automatic dispute rights if any future payments are presented. The Provider states that as it is subject to a 120 day time period in relation to investigating transaction disputes, it will be unable to attempt to dispute transactions for those merchants on behalf of the Complainant. The Provider notes that these dispute transaction rules are not set by the Provider but are these are Visa or MasterCard rules which the Provider must adhere to. The Provider recommends that the Complainant contact the merchant in question if he believes that the subscriptions did not belong to him and they may offer a refund.

In regard to the transactions on the account appearing in US or GBP, the Provider states that these are standard bank charges which occur when a point of sale transaction in a different currency is being made.

In response to questions raised by this Office, the Provider highlights a series of phone calls between it and the Complainant in respect of suspicious account activity in 2018. It argues that on 2 April 2018, the Complainant's card flagged on its card security alert system for a transaction in the amount of €40 for the merchant "CumminsSportSporting". A temporary block was placed on the Visa debit card and messages sent to the Complainant to confirm if the payment was genuine. It states that the Complainant telephoned it in response and confirmed that he had completed the €40 transaction for the merchant in question. The Provider states that it advised the Complainant that there are two other transactions appearing on the account in the amount of €4.98 on 1 April 2018 and €21.99 on 31 March 2018 and that the Complainant confirmed the transactions were his. It submits that the Complainant confirmed those transactions were legitimately made by him.

/Cont'd…

The Provider states that on 29 May 2018, the Complainant's card flagged again on the card security alert system for a transaction in the amount of €12.29 under merchant reference "expgmp.com". The Provider issued an SMS and email to the Complainant requesting confirmation that the transaction was genuine and states that the Complainant responded by SMS confirming the transaction as genuine so the temporary block was removed from the card.

The Provider states that on 6 July 2018, the Complainant's card flagged on the card security alert system for a transaction in the sum of €39.48 in relation to merchant name "DPLOOK.COM Direct Marke". The Provider states that it sent an SMS and email to the Complainant and placed a temporary block on the Complainant's card but the Complainant did not respond. On 14 July 2018, it states that the Complainant telephoned it in relation to difficulties he was experiencing with his card and was informed that the card was temporarily blocked pending a response by him to a security alert issued on 6 July 2018. The Provider advised him about the transaction that was pending and asked if the Complainant knew anything about it. The Provider states that the Complainant confirmed that he did but that it was the merchant's second time to try to take the money and asked if there was a way to stop this. The Provider asked if the Complainant had signed up for this and the Complainant confirmed that he was on the website of the merchant but didn't sign up to it. The Provider indicated that the Complainant must have provided his card details as the merchant could not debit his account without the 16 digit card number. The Provider states that the Complainant confirmed that he had provided his card details but asked if there was something he could do about it. The Complainant was encouraged to call the Provider when he got home in respect of transactions appearing on the account as the reception was poor and he was advised that there appeared to be quite a number of transactions, all in relation to dating websites that it appeared that he had signed up for. The Provider states that the Complainant acknowledged this and asked why his card was not working. He confirmed that the transaction from 6 July 2018 was legitimate. The Provider states that the Complainant did not contact the Provider to discuss the transactions appearing on the account after being advised to do so on 14 July 2018.

The Provider states that on 5 October 2018, the card again flagged on the card security alert system for a transaction in the sum of €12.29 for merchant "SWEVEB.COM". The Provider issued an SMS and email to the Complainant requesting confirmation of the transaction made and received a confirmation from the Complainant.

The Provider states that on 10 January 2019, the Complainant contacted it by telephone in relation to transactions which he did not recognise on his current account. He highlighted a number of payments from the previous year from the merchants "PFA*Hong C SM" and "SWEVEB.COM". When asked if he had received notifications about the transactions, the Complainant responded that he was not sure but he doubted it. In the course of this phone call, the Complainant confirmed that he did not check his account regularly. He further indicated that there are more unauthorised transactions going back to 2014.

/Cont'd…

The Provider explained that it would be extremely difficult to investigate transactions going back that far and that he may have been signed up for a subscription based company without his knowledge. The Provider advised the Complainant that if his card details had been compromised by a fraudster, his account would have been cleared out by now.

The Provider argues that it informed the Complainant that any transactions over 13 months could not be taken on as fraud and could not be investigated further. The Provider argues that the Complainant only raised concerns to the Provider in January 2019 so any transactions being disputed by the Complainant between 2013 and 2018 fall outside the timeframe of 13 months.

The Provider highlights clause 12 of its terms and conditions which provides that any transactions that are disputed by a customer must be brought to the Provider's attention as soon as possible "*but no later than 13 months after the date of the transaction*".

The Complaint for Adjudication

The complaint is that the Provider allowed payments to be made from the Complainant's account without his knowledge or authorisation, and authorised payments by third party merchants without noticing suspicious activity.

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.

/Cont'd…

A Preliminary Decision was issued to the parties on 10 May 2021, outlining my preliminary determination in relation to the complaint. The parties were advised on that date, that certain limited submissions could then be made within a period of 15 working days, and in the absence of such submissions from either or both of the parties, within that period, a Legally Binding Decision would be issued to the parties, on the same terms as the Preliminary Decision, in order to conclude the matter.

In the absence of additional submissions from the parties, within the period permitted, I set out below my final determination.

The Provider maintains a security alert system which monitors card transactions on customer accounts and raises an alert for any transaction that is deemed "suspicious". In those circumstances, the transaction will be flagged for further investigation and the Provider will contact the cardholder by SMS and email requesting the cardholder to confirm or decline the transaction.

The Provider will place the card on a temporary block pending confirmation that the transaction in question was genuine. This procedure is set out in the Provider's terms and conditions at clause 6.6.

The Provider states that the Complainant's Visa debit card was flagged on four occasions in 2018 – 2 April 2018, 30 May 2018, 6 July 2018 of October 2018. On all four occasions, the Complainant confirmed that the transactions were legitimate.

On 2 April 2018, a transaction in the sum of €40 from merchant "CumminsSportSporting" was flagged by the Provider and a temporary block placed on the Complainant's card pending confirmation by him whether the payment was genuine or not.

The Complainant telephoned the Provider in response to the security message and confirmed the transaction in question. On the same call, the Provider advised the Complainant that there were two other transactions appearing on the account in the amounts of €4.98 on 1 April 2018 and €21.99 on 31 March 2018. The Complainant confirmed that both transactions were legitimately made by him. Both of these transactions were respect of merchant "PFA*HongC SM". A number of transactions from this merchant, including the transactions on 1 April and 31 March 2018, were highlighted by the Complainant in January 2019 as being unauthorised.

On 29 May 2018, the Complainant's card flagged on the Provider's card security alert system for a transaction in the amount of €12.29 from merchant "expgmp.com". The Provider issued an SMS and email to the Complainant requesting confirmation of the transaction was genuine. The Complainant confirmed via text message that this transaction was genuine and the temporary block was removed from his card. In January 2019, the Complainant highlighted transactions from this merchant as having been unauthorised.

/Cont'd…

On 6 July 2018, the Complainant's card flagged on the Provider's current security alert system in respect of a transaction in the sum of €39.48 relating to merchant "DPLOOK.COM Direct Marke". The Provider issued an SMS and email to the Complainant and placed a temporary block on the card. The Complainant did not respond to the security alert message. The Complainant telephoned the Provider on 14 July 2018 in respect of difficulties he was experiencing using the debit card while travelling on a ferry. The Complainant was asked if he knew anything about the transaction and the Complainant confirmed that he did, but it was the second time the merchant was trying to take money and asked if there was a way to stop this. The Provider asked if the Complainant had signed up for this web service and the Complainant confirmed that he had been on the website of the merchant in question but did not sign up for it. The Complainant confirmed that he had provided his card details to the merchant in question. The Provider advised the Complainant that there appeared to be a number of transactions which looked as if he had signed up for a few dating websites which were trying to take money from him. The Complainant did not deny this and asked why his card was not working. The Provider explained that the card was blocked as he had not responded to the security card alert message on 6 July 2018. The Complainant asked for the card to be unblocked and the Provider confirmed it could be unblocked if the Complainant confirmed that the transaction was genuine.

The Complainant confirmed that transaction was genuine and the Provider removed the temporary block. As the reception on the call was poor, the Provider encouraged the Complainant to call the Provider when he got home to go through the various transactions. The Complainant failed to follow up with the Provider following this call.

On 5 October 2018, the Complainant's debit card was flagged on the Provider's card security alert system for a transaction the amount of €12.29 for merchant "SWEVEB.COM". The Provider issued a security alert message to the Complainant requesting confirmation of the transaction was made by him. The Complainant confirmed the transaction by responding 'yes' to the Provider and the temporary block was removed from his card. On 9 October 2018, there were 7 credits in the amount of €12.29 made to the Complainant's current account from merchant "SWEVEB.COM".

The Complainant cancelled his Visa debit card on 9 January 2019 and had a number of phone calls with the Provider on 10 January and 14 January 2019 in which he disputed a number of transactions. The specific transactions discussed on those calls were payments made to "HC Hong" for €4.98 and €21.99 and €2.60 in early April 2018. As mentioned above, the first two of these three transactions had been confirmed as genuine by the Complainant on a phone call with the Provider on 2 April 2018. The parties also discussed transactions from the merchant "SWEVEB.COM" and the Provider highlighted that 7 of the 9 transactions during 2018 from this merchant had been re-credited to him on 9 October 2018. As noted above, the Complainant had confirmed a transaction from that merchant on 5 October 2018 as genuine. The Complainant notified the Provider that there was a large number of transactions dating back 2014 which were unauthorised and which had only just come to his attention.

/Cont'd…

Under the terms and conditions of the Complainant's current account, clause 12 provides as follows:

> "12.2 *You must tell us about any transaction that was not (a) authorised by you or on your behalf … as soon as possible but not later than thirteen months after the date of the transaction*."

This 13 month time period corresponds with the time period laid down in the European Communities (Payment Services) Regulations 2009 (**PSR 2009**) and European Communities (Payment Services) Regulations 2018 (**PSR 2018**).

Under PSR 2018:

> "93. (1) A payment service user entitled to use a payment instrument shall—
>
> (a) use the payment instrument in accordance with the terms governing the issue and use of the payment instrument, which must be objective, non-discriminatory and proportionate, and
>
> (b) notify the payment service Provider concerned, or an entity specified by the latter for that purpose, without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.
>
> (2) For the purposes of paragraph (1) (a), the payment service user concerned shall, in particular, as soon as it is in receipt of a payment instrument, take all reasonable steps to keep its personalised security credentials safe.
>
> 95. (1) A payment service user is entitled to rectification of an unauthorised or incorrectly executed payment transaction from a payment service provider only where the payment service user notifies the payment service provider without undue delay on becoming aware of any such transaction giving rise to a claim, including a claim under Regulation 112, and no later than 13 months after the debit date.
>
> 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.
>
> . . .

/Cont'd…

(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.

Comparable provisions are contained in PSD 2009, with a 13 month period for notification of unauthorised transactions appearing in Reg 72 and a maximum €75 limit provided under Reg 75 in respect of unauthorised transactions, other than those occurring with the fraud or gross negligence of the payment instrument user.

With the above contractual and legislative provisions in mind, there are two main questions arising for determination:

1. Was the Provider entitled to disregard notification in January 2019 in respect of allegedly unauthorised transactions which occurred between 2014 and 2018? and

2. Whether the Complainant is entitled to a refund of any transactions that he alleges were unauthorised by him and occurred during 2018?

In respect of the first question, I am satisfied that the Complainant was obliged to notify the Provider in respect of any unauthorised transactions as soon as possible and no later than 13 months after the transaction in question. On that basis, and as the first notification that the Provider received in respect of allegedly unauthorised transactions occurred on 10 January 2019, I accept that the Provider was not obliged to investigate or refund any allegedly unauthorised transactions which occurred prior to 10 December 2017.

In respect of the allegedly unauthorised transactions which took place between 10 December 2017 on 10 January 2019, I have reviewed the Complainant's bank statements and based on the suspicious transactions that he highlighted in his letter of complaint to the Provider dated 23 January 2019, the following transactions appear to be alleged to have been unauthorised by him:

- 2 April 2018 PFA*HONGC SM €4.98
- 1 April 2018 PFA*HONGC SM €21.99
- 1 April 2018 PFA*HONGC SM €2.96
- 5 June 2018 SWEVEB.COM €12.29
- 20 June 2018 SWEVEB.COM €12.29
- 5 July 2018 SWEVEB.COM €12.29
- 20 July 2018 SWEVEB.COM €12.29
- 4 August 2018 SWEVEB.COM €12.29
- 19 August 2018 SWEVEB.COM €12.29
- 3 September 2018 SWEVEB.COM €12.29

/Cont'd…

- 18 September 2018 SWEVEB.COM €12.29
- 3 October 2018 SWEVEB.COM €12.29

Of the 9 transactions taken by the merchant SWEVEB.COM in the sum of €12.29, 7 of these transactions were refunded on 9 October 2018. The total sum outstanding on the allegedly unauthorised transactions that occurred within the 13 month timeframe from notification is therefore €54.51.

In respect of three transactions which took place on 1 and 2 April 2018 by 'PFA*HONGC SM', the Complainant confirmed to the Provider on a telephone call dated 2 April 2018 that two of those three transactions were legitimate that is, that they had been authorised by him. While there was no mention during the phone call of the smaller transaction of €2.96, it is notable that this transaction was from the same merchant that the Complainant had confirmed as legitimate in respect of the other two transactions. Further, by text dated 5 October 2018, the Complainant confirmed a transaction from 'SWEVEB.COM' in the sum of €12.29 as legitimate. While there is no way to know whether this transaction that was confirmed by the Complainant was one of the 7 that were re-credited to his account or one of the 2 that were not, it is notable that a transaction from the merchant in question was confirmed as legitimate by the Complainant.

From my review of the available evidence including the audio recordings of telephone calls between the parties, I further consider the following to be relevant to the question of Complainant's entitlement to a refund in respect of the allegedly unauthorised transactions:

1. On a telephone call on 14 July 2018, the Provider highlighted to the Complainant that there were a number of transactions appearing on his account, all of which appeared to be related to dating websites and which were attempting to take money from his account. The Complainant was encouraged to contact the Provider as soon as he got home (he was on a ferry at the time) to further investigate these transactions. Despite the Provider having flagged these transactions to the Complainant, he appears not to have reviewed his bank statements and did not follow up with the Provider in this regard; and

2. On the same call on 14 July 2018, and in respect of a transaction from a different merchant ('DPLOOK.COM') which has also been identified by the Provider as being a dating website, the Complainant accepted that he had been on the website of the merchant and confirmed that he had provided the merchant with his 16 digit card number, though denied he had signed up with it.

The following is of particular note:

(i) The Complainant's confirmation to the Provider in 2018 that transactions from each of the merchants in question were legitimate,

(ii) The Complainant's confirmation to the Provider that he had been on a comparative website and had provided his 16 digit card number to that merchant; and

/Cont'd…

(iii) The Complainant's failure to follow up with the Provider after the call on 14 July 2018 when the Provider had identified a number of transactions appearing on his account in respect of such websites and encouraged him to call it to further investigate the transactions,

The cumulative effect of these actions/inactions leads me to the inevitable conclusion that the transactions in question were either authorised by the Complainant (albeit that he may not have been aware that he was signing up for subscription services) or that he was grossly negligent within the meaning of PDS 2018 in respect of the transactions in question by proving his card details to the merchants in question and/or confirming that transactions from those merchants were legitimate when they were flagged as suspicious by the Provider.

In the circumstances, I do not consider the Provider to have been at fault or unreasonable for its refusal to compensate the Complainant in the sum of €54.51 in respect of the allegedly unauthorised transactions that occurred on the Complainant's account in 2018. As indicated above, the other transactions which were flagged by the Complainant as having been unauthorised fall outside of the 13 month timeframe within which he was obliged to notify the Provider of unauthorised transactions.

Further, it appears to me that the Provider's card security alert system was effective in 2018 in that it gave the Complainant a number of opportunities to accept or reject transactions with appeared to the Provider to have been suspicious. As the Complainant has subsequently sought to disclaim those transactions, it appears the Provider's concerns in this regard were justified. Finally, I am satisfied on the basis of the audio recordings provided to me that the Provider assisted the Complainant insofar as it was possible with his queries and handled his complaint appropriately.

For the reasons outlined in this Decision, I do not uphold this complaint.

Conclusion

My Decision pursuant to ***Section 60(1)*** of the ***Financial Services and Pensions Ombudsman Act 2017***, is that this complaint is rejected.

The above Decision is legally binding on the parties, subject only to an appeal to the High Court not later than 35 days after the date of notification of this Decision.

GER DEERING
FINANCIAL SERVICES AND PENSIONS OMBUDSMAN

1 June 2021

/Cont'd…

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

(a) ensures that—

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

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

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