



<u>Decision Ref:</u>	2021-0121
<u>Sector:</u>	Banking
<u>Product / Service:</u>	Debit Card
<u>Conduct(s) complained of:</u>	Disputed transactions Dissatisfaction with customer service
<u>Outcome:</u>	Rejected

**LEGALLY BINDING DECISION
OF THE FINANCIAL SERVICES AND PENSIONS OMBUDSMAN**

The complaint concerns the Complainant's debit card held with the Provider.

The Complainant's Case

The Complainant's expired debit card for her account with the Provider was linked to a card network provider (the **CNP**) payment service. The expired card was recorded as a payment instrument on a third party's account with an online retailer.

According to the Complainant, the third party also had an expired card, from a third party bank, registered with the online retailer. The Complainant asserts that a debit was attempted by the online retailer against the third party's expired card. The debit was rejected by the third party bank. The Complainant asserts that the online retailer then sought payment from the Complainant's card which was expired for almost 2 years at that stage. On 2 November 2018, the Provider processed a payment of €2.99 to the online retailer on her new debit card. The Complainant asserts that the details of this new debit card had not been furnished by the Complainant to the online retailer. The Complainant maintains that she did not authorise the payment nor did she have a continuous payment instruction with the online retailer at any point.

The Complainant contends that the payment was taken without her permission and that when she requested a list of the online merchants that the Provider has the update arrangement with, the Provider has said it cannot provide such a list. The Complainant has also queried whether there is a timeframe on how long a card can be expired as part of the update program.

The Complainant indicates that the Provider's customer support told her that it is the CNP which determines the list of companies allowed to access the new account information.

The Complainant also argues that she has received conflicting information from the Provider in respect of the incident.

The Complainant asserts that no subscription was attached to the expired card while it was still valid, and the Provider allowed the transaction without her permission.

The Complainant has refused to accept the Provider's offer of compensation. She states that the issue still remains that while her card was valid, she had no subscription service with the online retailer in question. She argues that the Provider allowed a brand-new subscription to charge her account despite her card being expired for a considerable period of time. She states that she was in contact with the CNP at the very outset of the complaint. It informed her that their automatic updater programme was not applicable in this instance and the fault was with the Provider. Despite having relayed this information to the Provider at the time and on other occasions since, she argues that the Provider has insisted on laying the blame with CNP's updater programme.

The Complainant wants the complaint to be reviewed by this Office so that the Provider will recognise and admit its fault, which it has not done in her view.

The Provider's Case

The Provider argues that it issued the Complainant with a new card in May 2017 as her card was due to expire at the end of May 2017. In respect of the process of updating new card details, the Provider states that when a cardholder's card is due to expire, a new card with the same card number but a later expiry date is generated on its card system. The Provider states that it issues an electronic file with updated card details to the CNP, with the card number and expiry date only. It states that this is required as part of the Visa Account Updater (VAU) programme that the Provider is obliged to be a part of as a member of the CNP network. It argues that merchants who are members of the VAU programme can then request these updated details from the CNP, through their own acquiring bank. The Provider states that it is not in a position to establish if the online retailer in this case was enrolled as a member of the VAU programme or not as the agreement is one between the CNP and the member merchant's bank.

The Provider argues that it did not update the card details with the online retailer. It states that it only updates these new card details with the CNP when a new card is issued. The Provider acknowledges that in its final response letter dated 27 November 2018, the Provider was incorrect to advise the Complainant that her details had been updated with the online retailer through VAU. The Provider states that it is not aware of whether or not the online retailer is a member of the VAU programme. The Provider apologises for this incorrect information given to the Complainant in its final response letter.

In respect of its inability to cancel the transaction in question, the Provider refers to its Debit Card Terms and Conditions of Use. In respect of Condition 3.4 which notifies cardholders of continuous payment instructions, the conditions of use provided as follows:

“We cannot cancel a Transaction that you have authorised. If you have a continuous payment instruction (for example, a subscription, set up from your Card with a third party) and you want to cancel it you can do so by contacting us up to the last Business Day before the payment is due to leave your Account. You should also give written notice to the third party and keep a record of any contact made.”

In respect of the Provider’s obligations of membership with the CNP which is a global payments technology company, the Provider states that it moved to debit cards issued through the CNP in 2012. It argues that the Complainant was provided with a CNP debit card in July 2015. It states that the Complainant’s card was attached to a card mailer advice document which explained to the Complainant that the new debit card was operated under the CNP Debit Card scheme. It argues that this card mailer document set out the benefits of the new CNP Debit cards, advice on using the card, and the terms and conditions that apply to it.

The Provider argues that by using the card, the Complainant was deemed to have accepted the Terms and Conditions of the card. It points to the card mailer advice document that issued to the Complainant which stated that: *“The use of your Card is governed by the terms of the Agreement. By using your Card you are deemed to have accepted the terms of the Agreement”*. It further pointed out that the card mailer document indicated that the card was operated under the CNP Debit Card Scheme. It argues that “Scheme” was defined in the Terms and Conditions as *“a third party payment system which manages and controls the processing of Transactions in accordance with its rules.”*

The Provider accepts that it does not advise cardholders of the VAU programme in its terms and conditions or offers them the choice to opt out of it. It states that the terms and conditions are currently being reviewed by the Provider and this will be considered as part of that review. The Provider states that if the cardholder would like it to remove them from the process of updating the details through VAU, it can do this on their request but it is important to note that by doing this, the onus will be on the customer to engage with the merchants directly if they change card numbers. The Provider cannot guarantee what action the merchant could take on receipt of an opt-out response under the VAU and could, for example, decide not to proceed with the transaction, thus impacting the service the cardholder expects to receive. The Provider states that it should have advised the Complainant of this opt out option in its final response letter and apologises for this omission.

The Provider states that it is not on notice of any continuing payment instruction with any particular merchant as these agreements are between the cardholder and the merchant. The Provider states that it merely acts as a facilitator for the transactions. The Provider states that it merely updates the CNP with the updated card details under the VAU programme and not individual merchants.

/Cont’d...

The Provider states that when it receives an authorisation request from a merchant, this is approved or declined in the standard manner, depending on the details provided by the merchant when processing the transaction.

The Provider states that the disputed transaction was subject to the European Communities (Payment Services) Regulations 2018 (**PSR 2018**). The Provider states that the terms and conditions applicable to the debit card comprise the framework contract applicable under the PSR 2018. It states that it was incorrect to tell the Complainant that the online retailer had used the up-to-date card details obtained through the VAU programme as it has no way of confirming this. It argues that it followed the terms and conditions in relation to unauthorised transactions and reported the transaction within the appropriate timeframe in line with condition 3.5 of the debit card terms and conditions. The Provider argues that the Complainant was provided with a copy of the terms and conditions of the card on each occasion that the card was sent to her. The Provider relies on Condition 28 which advised the Complainant of what was required to stop any further transactions where she may have set up a continuous payment instruction as follows:

“Where you have authorised the Merchant to set up a continuous payment instruction on your Card and you wish to cancel it, you must send a written cancellation notice to the Merchant and keep a copy of the letter. Service of such a cancellation notice on a Merchant shall not constitute, or be deemed to constitute, service of any such notice on us.”

The Provider argues that it had removed the requirement for cardholders to send a written cancellation notice to the merchant by the time the disputed transaction took place. The Provider also sets out various conditions providing safeguards and security measures in relation to the card and the Complainant’s obligation to ensure the safety of the card and to notify the Provider if she believed the details to be compromised. The Complainant’s liability was outlined in the terms and conditions as follows:

“If you use your Card as a Consumer, your liability will be limited to an overall limit of €75 for any losses incurred in respect of unauthorised Transactions arising from the use of a lost or stolen Card or from a failure to keep personalised security features safe.”

The Provider states that when the disputed transaction had taken place, this liability had been reduced to €50. The timeframe for cardholders to notify it of unauthorised transactions was outlined in Section 20 of the terms and conditions as an obligation to immediately report such transactions and any event within 13 months of the transaction being debited. The Provider argues that it complied with Regulation 81 in respect of the disputed transaction and details of the transaction were available to the Complainant on her online banking and bank statements. It argues that the details include the merchant’s name, and the date and value of the transaction.

The Provider argues that when the Complainant contacted it, the Complainant advised that she had previously provided her card details to the online retailer and her details were saved with the online retailer.

/Cont’d...

On that basis, the Provider asserts that it could not consider the transaction to be unauthorised as the Complainant may have entered into a continuous payment instruction with the online retailer in question. It states that the transaction was placed into dispute and referred to its chargeback team. When the chargeback team began their investigation, it was noted that the online retailer had refunded the transaction on 12 November 2018 and the dispute was closed. The Provider notes that the final response letter informed the Complainant of the refund transaction. It accepts that the refund from the online retailer was not at the request of the Provider.

The Provider states that it did not notify the Complainant that the debit card may automatically update in third party merchant sites that she had used previously when a new card was issued to her. Separately, however, it states that Continuous Payment Instructions are referenced in the Terms and Conditions of the debit card in Condition 3.4. In respect of the potential timeframe for how long a card can be expired and still be part of the VAU programme, the Provider states that it only issues the updated details to the CNP when the card is re-issued. It states that it provides updated card details to the CNP on a continuous basis. These details are then sent from the CNP to an acquiring bank following a submission from the acquiring bank on behalf of their merchant (if the merchant is enrolled in the VAU programme) with the existing card details held on the merchant's file to identify where card details need to be updated on the merchant's records. The Provider argues that in accordance with Condition 3.4, the Complainant can cancel any payments up to the last business day before the payment is due to leave your account if you no longer wish to pay for the particular services.

The Provider argues that it cannot provide a list of online merchants that the Provider has the VAU arrangement with as it does not have an arrangement with any online merchants. The online merchants have an arrangement with the CNP and it is obliged to provide the CNP with updated card details for the purposes of the VAU programme to ensure there is no disruption of service for cardholders.

The Provider acknowledges that it gave the Complainant conflicting information in relation to the transaction and apologises for this. The Provider argues that it cannot provide the CNP's processes for the VAU process due to a confidentiality clause with the CNP.

The Provider states that when the Complainant raised a complaint with it, the relevant reports were not captured within the complaint file due to human error. It states that due to the timeframe that had passed, the required reports were no longer available for review of the transaction. More detail was provided when the complaint was raised with this Office. The Provider states that this issue was raised with the original complaint handler to avoid a recurrence of the issue. By way of apology to the Complainant and recognition of the service failings identified, the Provider offered a goodwill gesture of €1,000 to the Complainant in full and final settlement of the complaint. The Provider also offered the Complainant the opportunity of being removed from the VAU programme.

In a more recent submission, the Provider accepts that it was incorrect to advise the Complainant that her details were updated through the VAU programme and states that it has apologised for this. The Provider further accepts that there were failings in the service provided to the Complainant in that she was given conflicting information in relation to the transaction and apologised for this also.

The Complaints for Adjudication

The complaint is that the Provider wrongfully allowed the processing of a payment transaction on the Complainant's account using the Complainant's debit card without her consent. Further, that when asked for information in relation to the basis of its right to do so, the Provider wrongfully failed to furnish the requested information.

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 5 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 Provider made a submission under cover of its e-mail and attachment to this Office dated 23 November 2020, a copy of which was transmitted to the Complainant for her consideration.

/Cont'd...

The Complainant has not made any further submission.

Despite the fact that the Provider in this case has submitted a detailed response to the complaint and responded to the questions raised by this Office, there are a number of matters which are still unclear.

I have no evidence as to whether the merchant in question (the online retailer) was ever authorised by the Complainant or the third-party to set up what is known as a continuous payment instruction. It is accepted by the Complainant that her expired card details were given to the online retailer some years ago but there is no information on what exactly was authorised at that time. It is clear that the Complainant is of the view that there was not a continuous payment instruction. The Provider has indicated from the outset that the transaction appeared to be as a result of a continuous payment instruction.

However, as there is no evidence available from the merchant in question, the third-party or the Complainant, it is not possible to come to a definitive conclusion on this matter. That said, I have no reason to doubt the Complainant's recollection.

The lack of information in this regard, is of concern. It is worrying that the Provider would rely on presumptions in relation to such a debit. As a result, it is difficult for me to determine whether the transaction in question could be regarded as properly authorised or was unauthorised. Further, even if it was not authorised by the Complainant and/or her agent, the fault in respect of seeking the payment of €2.99 in November 2018 would fall with the merchant in question, who I note refunded the transaction after several days.

The key issue is that I have not been provided with clear information on the payment instruction received by the Provider that led to it authorising the transaction in question. I note that the Provider has indicated that due to human error, the record in question was not retained by the individual looking into the complaint and that by the time the complaint was received through this Office, the record was no longer available. This position is obviously unsatisfactory, but I note that the Provider has accepted its fault in this regard and states that it has taken steps to ensure that the situation will not arise again. Recordings of telephone calls between the Complainant and the Provider have been furnished in evidence. I have considered the content of these calls. Based on one of the three recorded telephone calls from 9 November 2017, I note that the Provider suggested that the online retailer "*forced through the transaction without an expiry date*". In other accounts, it placed blame on the automatic updated programme. As I have no further information in relation to this, I cannot make a finding in respect of the appropriateness of the authorisation of the transaction in question based on the payment request received through the CNP by the Provider.

I am unclear whether the online retailer in question used the Complainant's expired card in seeking payment for the disputed transaction or whether it used the Complainant's new card having received updated card details through the card network provider (CNP) in question.

/Cont'd...

As it should not be the case that the merchant can utilise an expired card to receive payments, I am of the view that I have to proceed to consider the present complaint on the assumption that the CNP provided updated card details in respect of the Complainant to the merchant in question. I am dissatisfied with the clarity of the Provider's response in this regard. Again the key issue is the lack of information available from the Provider.

I consider the nub of the present complaint to be the level of information provided or not provided to the Complainant in respect of the automatic updating of her card details through the CNP in question and the lack of information in relation to the authorisation of the payment. This complaint has arisen because of the information provided to the Complainant and the information not provided to her at the time that her debit card was issued to her and also when she attempted to dispute the transaction in question.

The automatic updater programme (**VAU**) is explained on the CNP's website in the following terms:

"Increase authorisation approvals and reduce customer service issues and expense. VAU offers two solutions that help allow you to manage recurring payments and card-on-file relationships more efficiently and to reduce authorisation declines, so you can deliver a more positive customer experience; VAU and Real Time VAU.

Each solution has unique capabilities, but both provide automatic account updates to merchants and acquirers.

Merchants enrolled in VAU receive updates to cardholder account information, including new account numbers, new expiration dates, and/or contact cardholder notifications from participating Visa issuers."

On this account, it appears that it is up to each card issuer to choose whether or not to sign up to the two solutions offered by the CNP that is, the VAU and/or the Real-Time VAU. The Provider has indicated that it is forced to operate the VAU programme, though this is not borne out by the CNP's website information. In a fact document on the website, the following is stated:

"Please note, these two solutions are not mutually exclusive, so it's recommended that merchants, issuers, and acquirers participate in both solutions. In either case, cardholders don't always have to update their payment information and merchants can manage account information with ease. By delivering this time-saving efficiency, you create value for each stakeholder in the payment process."

The document supports the Provider's submission that as the card issuer, the Provider simply updates the CNP with the new card details of each cardholder when an old card has expired and the CNP itself updates relevant merchants with the relevant card information though the merchants' acquiring banks. The CNP's Core Rules and Product and Service Rules document run to almost 900 pages.

/Cont'd...

I will now set out the chronology of events in respect of this dispute:

- 2 November 2018 – transaction with the online retailer approved by the Provider
- 5 November 2018 – transaction of €2.99 debited from the Complainant’s account
- 8 November 2018 – SMS fraud alert issued to the Complainant to confirm a separate transaction
- 9 November 2018 – call (**call 1**) received from the Complainant who confirmed all transactions from 1 November 2018 to 9 November 2018 to remove the security hold, including the transaction with the online retailer
- 9 November 2018 – second call (**call 2**) received from the Complainant expressing unhappiness that the online retailer transaction had gone through on her new card. A complaint was logged and the transaction placed into dispute
- 9 November 2018 – call (**call 3**) made to the Complainant from the Provider to provide an update in respect of the disputed transaction
- 12 November 2018 – the online retailer refunded the transaction of €2.99 to the Complainant’s account
- 15 November 2018 – disputed transaction removed from the Provider’s chargeback dispute queue as the merchant had refunded the account. A complaint acknowledgement letter was sent to the Complainant.
- 27 November 2018 – complaint final response letter sent to the Complainant.

Insofar as the Provider’s Debit Card Terms and Conditions are relevant to the dispute, acceptance of the relevant Terms and Conditions is set out in Condition 1.2. This provides that: *“By using your Card, we will consider this to mean that you have read and accepted the terms of this Agreement”*. *“Safeguard System”* is defined as *“a system to aid in securing use of your Card over the Internet . . .”* *“Security Details”* are defined as *“any security process you follow or use to make an instruction or confirm your identity (for example, pass code, password or fingerprint). . .”*

In Section 3 entitled *“Authorising Transactions”* the following appears:

“How do you authorise Transactions?”

3.1 The way you authorise Transactions depends on how you use your Card. You can:

- (a) use your Card with its PIN, for example a cash machine or other card terminal (for example, in a shop);*
- (b) use your Digital Wallet with or without your Security Details and/or a Safeguard System;*
- (c) provide the Card details by phone, mail or online, with or without the use of your Security Details and/or a Safeguard System;*
- (d) use your Card and/or Device for Contactless Transactions, where possible;*
- (e) use your Card together with your Security Details to transfer money to another card, where possible; or*
- (f) use your Card and sign for the Transaction.*

/Cont’d...

When you use your Card in these ways we will take it that you have authorised the Transaction.

Important: With some of the above, you may also be asked to use your PIN and/or to provide identification details, such as your name, address and telephone number, or call out parts of your Card details such as the 3 digit code on the back of your Card as a precautionary measure.

What affects how you authorise Transactions?

3.2 You must also comply with any additional terms connected with the use of your Card. These may be our terms and conditions (like those for a Safeguard System) or Third Party Agreements (such as those from the Provider of the Digital Wallet). If you don't comply, we might not authorise the Transaction.

...

3.4 We cannot cancel a Transaction that you have authorised. If you have a continuous payment instruction (for example, a subscription, set up from your Card with a third party) and you want to cancel it you can do so by contacting us up to the last Business Day before the payment is due to leave your Account. You should also give written notice to the third party and keep a record of any contact made.

Unauthorised Transactions

3.5 Except as set out in the rest of this "Unauthorised Transactions" section, if you notify us without undue delay the Transaction from your Account was not authorised by you, we will usually refund the amount of that Unauthorised Transaction and restore your Account to the state it would have been in had the Unauthorised Transaction not taken place. We will not have any further liability to you in this respect."

My reading of Section 3.1 of the Terms and Conditions suggests that the way in which the disputed transaction in this complaint was authorised – likely through the use of the automatic update program through the CNP – was not one of the listed methods of authorising transactions as the Complainant did not *"provide the Card details . . . online"* at the time of the transaction, but rather had provided older, then expired card details. Prima facie, therefore, it would appear that the transaction was not authorised appropriately under the Provider's relevant terms and conditions. These terms and conditions referred to Third Party Agreements but not specifically to agreements on how cards issued under the CNP's scheme would operate if different from the Provider's terms and conditions. There is no specific mention of the CNP, other than in reference to enhanced security safeguard systems.

/Cont'd...

I note that the Terms and Conditions provide that the extent of the Provider's liability in respect of an unauthorised transaction is the amount of the transaction in question. In the present case, there is no dispute that the merchant (that is, online retailer in question) refunded the disputed transaction and so no loss was suffered by the Complainant.

The letter sent to the Complainant enclosing her new debit card in 2017 provides as follows:

"Do I need to update my card details with anyone?"

If your card has been replaced, the number may be different so you'll have to update anyone that you've registered the card with, such as utility companies or insurance companies to ensure future payments."

This letter contained Debit Cards Terms and Conditions of Use effective from 6 December 2016.

In a 'card mailer document' sent with the Complainant's expired card in 2015, the Provider indicated that the card was issued under the CNP's scheme. "Scheme" is defined in this and the 2017 letter as "a third party payment system which manages and controls the processing of Transactions in accordance with rules".

Section 2 sets out the ways in which a transaction can be authorised including "2.2 use of your Card for Transactions by mail, telephone, mobile phone or other portable device, internet or by use of a Secure System". Condition 28 provides as follows:

"Once authorised by you, a Transaction cannot be subsequently revoked (whether or not voucher is signed or PIN verified). Where you have authorised a Merchant to set up a continuous payment instruction on your Card and you wish to cancel it, you must send a written cancellation notice to the Merchant and keep a copy of the letter. Service of such a cancellation notice on a Merchant shall not constitute, or be deemed to constitute, service of any such notice on us."

The Provider has argued that these letters indicate that the card was operated under the CNP Debit Card Scheme and that "Scheme" was defined in the Terms and Conditions as "a third party payment system which manages and controls the processing of Transactions in accordance with its rules." While this is the case, there is no relevant information set out or any term or condition from which a reasonable person on receipt of a new debit card could possibly be informed that the stated terms and conditions of the Provider were not the full picture and that a second, undisclosed set of rules applied by the CNP itself also dictates how transactions will or will not be authorised.

The Provider accepts that it does not advise cardholders of the VAU programme in its terms and conditions or offer them the choice to opt out of it. This is clearly the case. There is no reference in any documentation sent to the Complainant to a separate set of rules operated by the CNP (other than the vague 'Scheme' definition above), and no copy of or link to any additional CNP rules provided.

/Cont'd...

A reasonable consumer, on receipt of the relevant documentation, could have no reason to think that there was another set of CNP rules that would dictate something as important as the automatic updating of their card details with a merchant in existence. In respect of the VAU programme, the letter from 2017 expressly informs a cardholder to update card details with merchants to ensure future payments. There is no mention of the possibility of the card details being automatically updated.

I am not satisfied, therefore, that the Complainant was informed of the VAU programme in advance of using either of her cards.

In terms of the complaint itself, I note that on the first call that took place on 9 November 2018 (call 1), the Complainant expressly confirmed that the transaction for €2.99 with the online retailer was her transaction. On call 2, the Complainant rang to indicate that the online retailer had taken the payment from a card that had expired and that she had never updated the online retailer with her new card details but the Provider had let the payment go through in any event. The Provider's representative in question explained that some merchants have new card details automatically transferred over where card details are saved. The Complainant indicated that she never authorised the Provider to do this and it was never explained to her that the Provider could automatically update her card details. It was explained to the Complainant that she had to remove her card details from the account with the online retailer.

The representative in question indicated that she would log a complaint and would look into the process of how updating works to provide further information to the Complainant.

On call 3 on 9 November 2018, the representative in question stated that it appeared that the online retailer in question had forced through the transaction without an expiry date. She indicated that she would try to cancel the transaction. When asked by the Complainant how the merchant in question had forced the transaction through without an expiry date, the representative indicated that she did not know. She also stated that she had made a mistake in the earlier call when she informed the Complainant that her card details had been updated through the VAU programme as this was not the case. The Complainant was again advised to ensure that the card details were removed from the video account in question as the transaction was coming up as a continuous subscription so it needed to be removed.

By email dated 9 November 2018, the Complainant wrote to the Provider to make a formal complaint in relation to the processing of the payment from the expired debit card. In her complaint email, the Complainant argued that her old debit card had previously been used on an account with the online retailer and had expired in 2017. She indicated that she had been informed by customer services that her card details would be automatically updated by the Provider in certain cases. She argued that she did not give permission for the Provider to update her card details with any online merchant service and that this had never been explained to her in writing from the Provider.

In its final response letter to the Complainant dated 27 November 2018, the Provider stated as follows:

"I understand your complaint to be in relation to a transaction with [the online retailer] being processed in error to your card with your card details automatically updated.

...

Please note, [the CNP] is a global payments technology company of which we are a member. As a member, we are obliged to be part of the [automatic account updater or VAU] programme.

This programme enables enrolled merchants to obtain the latest card number and expiry date. The benefits are that it ensures the continuity of service for our customers by removing the inconvenience of manually updating your details and avoids a disruption of service ...

When your card details are provided by phone, mail or online, you may have set up a continuous payment instruction with the merchant. In line with condition 3.4 of the enclosed Debit Card Terms and Conditions of Use, we have placed a stop instruction on your account to prevent [the online retailer] from using your card details to process further instructions. I also confirm the transaction for €2.99 has since been refunded by [the online retailer].

We are sorry for any inconvenience caused to you as a result of this matter. Based on the above, I feel that [the Provider] are not at fault as they follow the normal procedures."

It is clear from the above, that there was confusion from the outset as to how the transaction in question was authorised. The first explanation is that the CNP provided the Complainant's updated card information to the merchant in question throughout the VAU programme and this allowed the merchant to seek payment despite having only been provided with the old, expired card details. This is the initial explanation provided in call 2 with the Complainant on 9 November 2018, and was the version that the Complainant set out in her complaint email of 9 November 2018, and the version that the Provider responded to by way of final response letter to the Complainant of 27 November 2018.

The second explanation is that provided in call 3 on 9 November 2018 in which the representative stated that the merchant is not part of the VAU programme and that it appears that the merchant had "forced through" the transaction in question without an expiry date. It appears on this explanation that the old, expired card details may have been used by the merchant as the card number remained the same but that the merchant did not use the expiration date in seeking payment. No explanation has been provided in respect of how such a transaction could have been authorised by the Provider.

/Cont'd...

In its response to queries raised by this Office, the Provider has submitted a third version of events – that it simply does not know whether or not the online retailer is a member of the VAU programme. It states that the previous information provided to the Complainant indicating that the online retailer had received updated card details through the VAU programme was incorrect as it does not, in fact, know whether this is true or not. The Provider has indicated that the transaction was placed into dispute with the chargeback team but as the online retailer refunded the transaction, it closed the dispute. In its response to this Office, the Provider has not even referred to the second explanation provided by its representative that the online retailer somehow forced the transaction through without an expiry date. As set out above, the Provider has accepted that the relevant reports were not captured with the complaint due to human error and, accordingly, transaction records are no longer available to examine the transaction in more detail.

The Provider's inability to explain exactly how the transaction in question was authorised is a matter of serious concern, regardless of the value of the transaction or the fact that the sum of money in question was refunded within a matter of days by the merchant.

Further, I am concerned by the inconsistent information that has been provided to the Complainant in respect of the disputed transaction. The Provider's response seemed to flip-flop between placing blame on the CNP automatic updater program and indicating that the merchant forced through the transaction without explaining how this was accomplished in the absence of an expiry date.

By its own admission, the Provider failed to give any indication to the Complainant that use of the debit card would engage CNP's automatic updater programme such that the new card details would be furnished from the Provider to the CNP and then from the CNP to any merchant with whom she had a continuous payment instruction in place. Whether or not there was a continuous payment instruction in place with the merchant in question in the present dispute, I am of the view that the Complainant was entitled to be informed of the existence of this VAU programme.

I note the Provider in its response to this Office has stated, that in addition to its goodwill offer it *"would also like to provide the Complainant with the opportunity of being removed from the Visa Update programme"*.

While I welcome this, I believe it would be far better if the Complainant, and card holders generally, were provided with an option to opt out of the VAU programme, if this is possible, when the relevant card is first supplied, rather than when an issue arises.

Under the Consumer Protection Code 2012 (CPC), the Provider is obliged to:

"2.6 make full disclosure of all relevant material information, including all charges, in a way that seeks to inform the customer;

2.8 correct errors and handles complaints speedily, efficiently and fairly;

/Cont'd...

10.11 maintain up to date and comprehensive records for each complaint received from a consumer."

I consider that these obligations were not complied with by the Provider owing to the fact that it failed to inform the Complainant of the existence and operation of the VAU programme; provided inconsistent information to the Complainant in respect of the complaint; and failed to maintain the appropriate records to properly explain how the transaction in question was authorised.

I believe that the information furnished by the Provider fell short of what the Complainant could reasonably have expected and what she should have been given.

The Provider failed to give an explanation for its authentication of the transaction in question; failed to notify the Complainant of the existence of the VAU programme. The Provider furnished inconsistent information to the Complainant in respect of the transaction and failed to maintain an appropriate record of the transaction in order to properly deal with the complaint.

I find it unacceptable that the Provider is unable to furnish any evidence to demonstrate whether the transaction in question was authorised or unauthorised. I note, however, that the transaction in question has been fully refunded so the Complainant is not at any loss in respect of the transaction.

I note the Provider offered the Complainant a "goodwill gesture" of €1,000 in full and final settlement of the complaint during the investigation of this complaint. The Complainant responded as follows:

"Having read and considered the response from [Provider] I have decided not to accept their offer.

The issue still remains that while my card was valid I had no subscription service with the 'video company'. The bank allowed a brand new subscription to charge my account despite my card being expired for a considerable period of time.

I was also in contact with visa at the very outset of this complaint who informed me that the automatic updater programme was not applicable in this instance and the fault was with the bank.

Despite having relayed this information to [the Provider] at the time and on other occasions since, they are insisting on laying the blame with Visa's updater programme.

I instigated this complaint with a view to [the Provider] recognising and admitting their fault, which has not happened."

/Cont'd...

I believe the “goodwill gesture” of €1,000 to be a reasonable sum of compensation. However, I also understand the Complainant’s frustration at not being able to secure the correct information from the Provider. Having a debit or credit card used, particularly online, in the manner in which the disputed transaction took place on the Complainant’s card can be very worrying. Being unable to get a clear and correct explanation greatly adds to the worry and inconvenience.

In my Preliminary Decision I indicated that, though I believed the compensation offered to the Complainant to be adequate, I proposed to substantially uphold the complaint and direct the Provider to review its conduct in relation to the information it provides to its customers regarding this service. I also indicated my intention to bring this Decision to the attention of the Central Bank. My concern related to the number of customers who could potentially be affected by the Provider’s failure to adequately inform its customers of (i) the existence and operation of the VAU programme, and (ii) the apparent ability of the customers in question to opt out of this service.

I note that the Provider, in its post Preliminary Decision submission dated **23 November 2020**, submitted to this office a copy of its updated terms and conditions and pointing out that:

“In light of the issues raised in the review of this complaint, the [Provider] wishes to advise that it has updated its Terms and Conditions governing Debit and Credit cards and these changes come into effect on 31 January 2021”.

The Provider details that as part of these changes, *“the [Provider] included additional information about the card updater service in which a card is automatically enrolled and advises that customers can opt out of this service by contacting the [Provider]”* and that *“these changes are presently being communicated to all card holders”.*

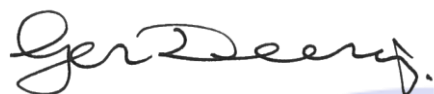
I welcome the action taken by the Provider in response to my Preliminary Decision. Having reviewed the subsequent actions of the Provider, and its acceptance of certain instances of fault in the above adjudication, I no longer deem it necessary to refer the matter to the Central Bank of Ireland.

Furthermore, as I believe the goodwill gesture of €1,000 offered by the Provider to the Complainant to be reasonable and on the basis that this offer remains available to the Complainant, I do not uphold this complaint.

Conclusion

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

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

28 April 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

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