DRN-4886012

The complaint

Complaint

A company, which I'll refer to as R is unhappy that chargebacks were raised against it after the 'Customer Not Present' (CNP) transactions it accepted turned out to be fraudulent. R believes that Elavon Financial Services Designated Activity Company (Elavon) are to blame for what happened because their security processes were flawed.

In bringing this complaint, R is represented by its director who I'll refer to as Mr C.

What happened

The facts of this case are not disputed. So, I'll briefly summarise them.

- On 17 October 2019, in order to facilitate card payment services, R entered into a Merchant Services Agreement with Elavon (the Agreement).
- On 23 and 24 August 2023, R accepted two card transactions for £893.24 and £2,487.35 for the sale of vehicle parts.
- The transactions were processed as CNP transactions.
- Unfortunately, the transactions turned out to be fraudulent. And were subsequently disputed by the genuine cardholder who said they neither authorised nor carried them out.
- In the event, Elavon attempted to challenge the chargebacks on the basis of evidence they received from R. But Elavon's challenge was unsuccessful.
- So, in October 2024 Elavon told R the chargebacks would stand. Believing this to be unfair, on R's behalf Mr C complained to Elavon.
- In his complaint, Mr C said Elevon had maintained that their process was a secure method for collecting payments. He believed Elavon should therefore accept responsibility for the charged back transactions because they resulted from a flawed security process.

Elavon didn't think they'd done anything wrong. In response to R's complaint, they said – in summary that:

- At all times Elavon acted in accordance with the relevant Card Scheme regulations and the terms of the Agreement. And ultimately in accordance with the Scheme rules, any transactions processed as CNP by R were carried out at R's own risk which is made clear in the Agreement that was signed by Mr C on R's behalf.

- In any event they attempted to challenge both chargebacks with the documentation that R provided. And they also asked for additional documentation aimed at proving that the card holder authorized the transactions.

- They made every effort to defend the two chargebacks by forwarding all the information R provided them with to the cardholder's bank. But the cardholder's bank rejected Elavon's challenge and confirmed that the transactions were fraudulent, and the cardholder did not participate in, or authorise them.

- Although R has maintained that the information it entered on the virtual system was verified, nonetheless any CNP transactions carry a risk. And an authorisation code for a transaction simply confirms sufficiency of funds and that the card presented has not been reported lost or stolen at the time of the transaction.

Our investigator didn't uphold the complaint. He didn't think Elavon made an error in this case. He was satisfied that Elavon had discharged their responsibility towards R by attempting to defend the chargebacks in that they sent the information obtained from R to the cardholder's bank. He explained that as Elavon were unsuccessful, this resulted in the cardholder being refunded by the amount of the disputed transactions.

The investigator wasn't persuaded that Elavon's security processes were flawed on the basis of Mr C's testimony. In other words that they failed to capture possible incorrect customer address details. He explained that it is the cardholder's bank rather than Elavon that has access to the cardholder's information for verification purposes.

The investigator agreed with Elavon that any CNP transaction presents a risk of chargebacks being raised. And as happened here, unfortunately in such circumstances it is the merchant – R - who is responsible for repaying the chargeback amounts should the chargeback decision go in favour of the cardholder.

Mr C didn't accept the investigator's conclusion. On behalf of R, he maintained his position that ultimately the chargebacks stemmed from flawed security systems on Elavon's part. By way of further explanation, he said in summary that:

- Previously R operated a manual terminal which was more secure than the 'virtual terminal' Elevon later introduced.

- In particular, in respect of the manual terminal, if an incorrect postcode or house number was put into the system a "no match" confirmation would be generated. In turn, R would not dispatch the goods being purchased without further contact with the customer.

- By contrast the virtual terminal did not perform in the same way in spite of information issued by Elavon affirming its security. In other words, Elavon wrongly asserted that the virtual terminal takes payments securely and that using it to process customers' payments meant this could be done with the benefit of full online security and fraud protection.

- In relation to the charged back transactions, the virtual terminal showed green ticks when the customers details were entered, indicating that everything was clear. The were no amber or red warning, either of which would have alerted R to withhold the goods. So, Elavon should assume responsibility for R's losses.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Where the evidence is incomplete or inconclusive (as indeed some of it is here) I reach my decision on the balance of probabilities – in other words, what I consider is most likely to have happened in the light of the available evidence and the wider circumstances.

For context I start by explaining briefly what a chargeback is.

A chargeback is the reversal of a previously cleared transaction. It is a process by which some disputes are resolved between card issuers and merchants under the relevant Card Scheme rules. And chargebacks are an unfortunate but inevitable consequence of on-line transactions.

It's important to note, however, that the decision whether or not to approve chargeback claims is for the Card Scheme to make and I'm unable to consider whether that decision is wrong or right.

It is also important to note that Elavon doesn't operate the Card Scheme or decide the success or otherwise of the chargeback. It has a specific role in the circumstances where a chargeback is raised which is only to decide whether or not to defend it.

Against that background, the question for me to decide is whether Elavon handled the chargeback request against R appropriately.

As I've just mentioned Elavon's responsibility during a chargeback dispute is to decide whether to defend it. And if they elected to defend it, they are obliged to represent R as fairly as possible - which includes providing the card issuer with all supporting evidence obtained from R in its defence.

It's not in dispute that when Elavon received documentation supporting the disputed transactions from R, on its behalf they defended the chargebacks with the card issuing bank. But that is an extremely difficult undertaking in cases of fraudulent transactions. In particular where the cardholder has said they were not responsible for carrying out the transactions.

That was at the heart of the card issuer's position when it declined to accept R's evidence. They didn't think R had provided evidence to show the transactions were indeed carried out or authorised by their cardholder.

I'm aware it is also part of R's case that the transactions were 'authorised' in light of the green ticks Mr C described as appearing on the virtual terminal - meaning R was not alerted against releasing the goods to the fraudsters.

But as Elavon has pointed out section 7 of the terms and conditions of the Agreement explains the effect of 'authorisation'. Having read the Agreement in full including the section just referred to, I'm satisfied it makes clear that acceptance of CNP transactions is done entirely at the customer's own risk.

And furthermore, that authorisation doesn't guarantee payment for a transaction or guarantee that the transaction won't be disputed at a later date given that all transactions are subject to chargebacks.

I think it's reasonable to conclude that having signed the Agreement on 17 October 2019, Mr C was aware or at least ought reasonably to have been aware that CNP transactions were not guaranteed. So, in the circumstances it is difficult for me to conclude that Elavon did anything wrong and should assume responsibility for the loss R has sustained.

I appreciate that R will be disappointed with that conclusion and what ultimately it means for the outcome of its case. And I understand and sympathise with what R has been through, particularly as the CNP transactions turned out to be fraudulent. However, having carefully considered the evidence I've seen from both parties, I'm satisfied Elavon have acted correctly within the Card Scheme rules to which they're bound, as well as the terms and conditions of the Agreement.

R now faces losses in excess of £3,300 for which I very much sympathise. But Elavon isn't liable for R's losses which were incurred due to an unfortunate fraud.

I've seen within the terms and conditions of the Agreement there is a specific section that explains that R is fully liable for any transaction that was returned to Elavon – including chargebacks and that the amount would immediately be repayable to Elavon.

What that means is that I'm unable to conclude Elevon has treated R unfairly in recovering from R the full amount of the transactions that were charged back. In the circumstances of this case therefore, since I do not find Elavon have treated R unfairly by their actions, I won't be asking them to take any further action.

Finally, I appreciate Mr C believes there is a flaw in Elavon's security process. In particular in the circumstances, he has described - including that Elavon's virtual terminal failed to identify the possibility of an incorrect address relating to the cardholder.

But like the investigator, it's not clear to me how reasonably that would be possible when it is the card issuer rather than Elavon who'd have such details. Rather, Elavon's checks were aimed at establishing whether the card in question was reported lost or stolen at the time of the transaction.

That being said, ultimately, the determining issue here is that these were CNP transactions in relation to which Elavon warned R of the risks involved. And as I've already explained I am unable reasonably to conclude they should be held responsible for R's losses which were incurred in consequence of those transactions.

My final decision

My final decision is that I don't uphold this complaint

Under the rules of the Financial Ombudsman Service, I'm required to ask R to accept or reject my decision before 3 October 2024.

Asher Gordon
Ombudsman