DRN-6131888

The complaint

Miss R is unhappy that Lendable Ltd trading as Zable refused to refund transactions she said she didn't authorise.

What happened

Miss R contacted Zable on 23 September 2024 to dispute 12 transactions totalling just over £550 carried out from December 2023 to May 2024 on her credit card.

Zable investigated Miss R's complaint and concluded the transactions were authorised so didn't offer a refund.

Zable's position is that all of the transactions were authenticated using 3D Secure (3DS) – an additional layer of verification in which the account holder approves the payment within their Zable app. Zable also noted that the transactions were made using two separate cards, one virtual and one physical, meaning a fraudster would have needed to compromise both which they felt was unlikely. As a result, Zable felt Miss R authorised the transactions.

Miss R has said her phone and physical card have remained in her possession but as she lives in shared accommodation, she couldn't rule out the possibility of someone accessing her phone, card or post. Miss R doesn't recall receiving any passcodes in the app and has said if she did, she'd have checked the transactions were authorised before continuing. Miss R also told us that she couldn't have made some of the payments because they were gambling transactions and Miss R had registered with a self-exclusion organisation (that I'll refer to as G) that prevented her from opening accounts with gambling companies. Miss R also questioned why gambling transactions were successful given they should be blocked on credit cards.

One of our Investigators recommended the complaint was upheld on the basis Zable had failed to evidence how the transactions were authenticated which was a requirement under the relevant legislation. They asked Zable to ...

Miss R accepted the Investigator's view, but Zable disagreed and asked for an Ombudsman to review things. In summary, Zable said that they'd provided evidence that the transactions were authenticated using 3DS in the app, that Miss R was logged into her app at the time of the transactions and she'd inputted 3DS on other transactions that aren't being disputed.

After reviewing the evidence, I reached a different outcome to the Investigator. I was persuaded Zable had shown how the transactions were authenticated and I ultimately concluded that the transactions were authorised by Miss R. So, I issued a provisional decision explaining my outcome.

Miss R disagreed with my provisional decision. Miss R reiterated that she didn't engage in the transactions and said someone must have accessed her details to carry out the transactions. Miss R also said that she couldn't identify any of the merchants from the information on her statements and questioned how an outcome could be reached without this information.

As Miss R didn't accept my provisional decision, I've reconsidered my findings below.

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.

In my provisional decision I said:

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

The Investigator's view was that Zable had failed to evidence how the transactions were authenticated and so Zable couldn't hold Miss R liable for the disputed transactions. Having reviewed all the evidence I've reached a different conclusion, and I'm satisfied Zable have demonstrated the disputed transactions were authenticated. I'll explain why below.

I've seen screenshots of Zable's internal system which show the payment method used for each of the 12 transactions. These screenshots coupled with other evidence from Zable's internal system show that the disputed transactions were online transactions authenticated using the relevant card details and 3DS. So, I'm satisfied authentication has been evidenced.

However, the relevant legislation states that authentication alone isnt sufficient for Zable to hold Miss R liable for the transactions. There must also be evidence that Miss R either made the transactions herself or authorised a third party to make them on her behalf.

Miss R has consistently said that she didn't authorise the transactions, so I've considered the likelihood of a third party being able to make the transactions without Miss R's consent or knowledge.

The evidence shows that the disputed transactions were initially made using Miss R's virtual card, provided when Miss R first opened her account with Zable, and later her physical card. As above, the evidence also shows that 3DS was successfully completed for each of the disputed transactions which required someone to log in to Miss R's Zable mobile app and approve each transaction. So, for a third party to carry out the payments, they would have needed to obtain both Miss R's virtual and physical card details as well as compromising the security on Miss R's phone and Zable mobile app.

Miss R has told us she lives in shared accommodation and so couldn't rule out the possibility of someone accessing her possessions without her knowledge, including her post, phone and cards. I appreciate what Miss R has told us about her post being left in a communal area and others having access to her room but that doesn't account for all the steps a third party would need to take to complete the transactions.

Miss R's virtual card was provided to her after her the successful application and the details were stored in her mobile app. So, a third party would have needed to obtain Miss R's phone which was stored in a locked room and then bypass the security on both Miss R's phone and Zable app. The third party would then need to repeat the same process again, on 12 separate occasions, in order to complete 3DS for each of the transactions. As for the later transactions made using Miss R's physical card, the third party would need to obtain Miss R's card details by accessing her card which was stored in a locked room. Alternatively, a third party would have needed to locate the letter containing Miss R's physical card and then opened and likely resealed the post so as not to arouse suspicion.

I don't find this was the likely the case. I say this because I'm not persuaded a third party would be able to accomplish all of the above without detection – not least because the third party would need to repeat this process multiple times over six months.

I must also consider the timeline of the transactions. We generally see fraudsters exhausting available funds as soon as they gain access to an account but in Miss R's case the transactions were relatively low value and spread over months. There was also a noticeable

delay between the transactions occurring and them being reported to Zable and I find it surprising that Miss R didn't report the disputed transactions sooner.

Miss R has shared with us that she used G which would have prevented her from making some of the transactions which appear to be to gambling websites. Zable don't have a responsibility to check G before allowing payments to go to gambling companies. Instead, G's self-exclusion system works on preventing customers from opening accounts with UK gambling companies. In any event, the transactions couldn't reasonably have been identified by Zable as gambling transactions because the transactions and merchants weren't identified in their system as gambling companies.

Overall, there's no plausible explanation for how a third party would be able to obtain both the virtual and physical card details, plus carry out 3DS on 12 separate occasions without Miss R's knowledge. So, on balance, I think Miss R more likely than not consented to the transactions and it's therefore reasonable for Zable to hold Miss R liable for them.

I'm afraid Miss R's response hasn't persuaded me to change my outcome.

The details available to Zable and Miss R won't always enable the merchant to be easily recognised as the merchant might use a legal name as opposed to a trading name. I note that Miss R has previously linked at least one of the merchants to a gambling company and I have linked some of the merchants to online game websites as well as what appears to be clothing and home brands. I appreciate Miss R's frustrations but want to assure Miss R that more details about the merchants wouldn't have led to me reaching a different outcome on whether the transactions were authorised.

Miss R has consistently said she didn't process the transactions and, whilst I have no reason to doubt what she's said, that's not enough for me to say the transactions weren't authorised by Miss R. I must also be persuaded that Miss R didn't give consent for the transactions, perhaps by sharing her card details or approving the transactions on behalf of someone else.

If Miss R wasn't involved in the transactions, a third party would have needed to compromise Miss R's virtual card, physical card and phone on more than one occasion without her noticing. As explained above, I've not been provided with a plausible explanation as to how this could have occurred and so I think it's more likely that the transactions were carried out with Miss R's consent and were therefore authorised.

My final decision

My final decision is that I don't uphold Miss R's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss R to accept or reject my decision before 5 March 2026.

Freyja Dudley
Ombudsman