DRN-3823148

The complaint

L, a limited company, is unhappy that GPUK LLP won't refund a transaction which it didn't authorise.

What happened

L operates a retail premises. A group of individuals approached the sales counter. They asked to purchase a number of products. In order to complete the purchase, they were given L's merchant terminal. Instead of entering a PIN to complete a transaction, one of the people was able to process a £999.99 refund to a debit card. L says that while one person pretended to enter their PIN, the others attempted to distract L's employee by enquiring about other products. One of the group claimed that there was a problem with the card purchase and they'd return with cash.

L didn't notice until a few days later, after which it reported the matter to GPUK. GPUK advised L to change the terminal password from its factory default and to inform the police. It said that it had contacted the card issuing bank but had been unable to recover L's money as there was no money available in the card holder's account.

The matter was referred to our service and one of our investigators upheld it. They thought that the processing of a refund in this way was a payment service under the Payment Services Regulations 2017 ("PSR 2017") and, therefore, L could only be held responsible for a transaction it had authorised. The investigator was satisfied (based on CCTV evidence and L's testimony) that wasn't the case.

They also thought that L hadn't breached Regulation 72 PSR 2017 (which, among other things, requires payment service users to take all reasonable steps to keep personalised security credentials safe) or the terms of the agreement as L's employee had been distracted by the fraudsters.

GPUK didn't agree. In summary it said:

- Responsibility for the terminal rested with the merchant.
- It had brought this particular risk to the attention of L – both in the Merchant Operating Instructions, in its Terms of Service and a leaflet entitled 'Know the Risks'. L's director had, in November 2021, signed a declaration confirming they'd read and understood those documents.
- It also relied on term 6.24 of its Terms of Service, which states: '*You must ensure that you are aware of the location of all terminals within your possession and periodically inspect devices to look for tampering or substitution. In addition you must ensure that all staff are trained to be aware of suspicious behaviour and to report tampering or substitution of terminals'*
- L didn't identify the transaction until two days after it took place – so L had acted negligently.
- It had highlighted the specific risk of customers interfering with the terminal in The Merchant Operating Instructions.

- The Merchant Operating Instructions and the 'Know your Risks' leaflet both have sections entitled 'Terminals' which explain that the customer is responsible for the terminal equipment and for any losses that arise from third parties using the machine, other than the way intended as part of the normal use of the machine. They also instruct the merchant to be wary of a customer who holds onto a terminal for longer than is needed to input a PIN.
- The fraudster would have needed to handle the card machine for a significant amount of time in order to process the transaction.
- So, overall, L was negligent in the way it used the equipment and GPUK couldn't be held responsible.

As no agreement could be reached, the case was passed to me for a final decision.
In advance of my final decision I contacted GPUK. I explained that I wasn't clear what its position was in relation to the PSR 2017, specifically whether it was of the view that L would be responsible for the loss, regardless of whether the payment was authorised by L or not.

GPUK responded to say that it did accept that the transaction was unauthorised, but that L had failed in its obligations under Regulation 72 of the PSR 2017, as it failed to abide by 72(1)(a) or 72(3). It cited the fact that a third party had processed a payment using L's terminal as evidence of this failure. It also argued that L had failed to 'establish a refund approval limit' on the terminal which, in its view, would have prevented the loss. Overall, it said that L hadn't shown reasonable care and GPUK could not have prevented the loss.

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.

Having considered this matter carefully I'm satisfied that:

- By providing merchant terminal services to L, GPUK was acting as its payment service provider.
- The refund was a payment transaction for the purposes of the PSR 2017.
- Under the PSR 2017 a payment service user isn't generally responsible for payment transactions it hasn't authorised.
- In this case, there isn't conclusive evidence that a third party made the payment – though I'm satisfied this is more likely than not to be the case based on CCTV screenshots and L's testimony. In any case, GPUK accepts that L didn't carry out the transaction and that there was no corresponding sale associated with the refund.
- Therefore I don't think the transaction was authorised by L, so, as a starting point, L should not be responsible for it, unless it can be shown that L acted with gross negligence or intent in failing to adhere to the terms of the agreement or Regulation 72, PSR 2017.
- Though GPUK have relied on the section of the Merchant Operating Instructions entitled 'Terminals', it accepts that a finding of liability should be dependent on whether it can be demonstrated that L failed in its obligations under Regulation 72.
- It's relevant to note that GPUK did not issue the payment instrument to L. It only provides merchant acquiring services. It also has no knowledge of whether additional security (such as a password) would have been required in order to process a refund (though it does recommend such a password is put in place).
- L has provided evidence of the specific terminal it was using at the time. I've reviewed the user guide for that terminal and it appears that a user would need to login to the device in order to process transactions, but no further security (such as a

password) would have necessarily been required in order for a transaction to be processed.

- Given that in order to process a sale through the terminal, an employee of L would need to be logged into it, it's evident that the action of handing over the terminal while it was in a state that a refund could be processed could not amount to gross negligence.
- It also means that L or its employees, would, on balance, not have had to disclose any security information or passwords for the refund to take place: it could have been carried out by anyone with a reasonable working knowledge of the machine and the opportunity to do so.
- I haven't been able to view CCTV footage of the events of that day, but I have seen stills of the alleged perpetrators. I understand that the retail premises is small – and it seems likely that the perpetrators would have been visible to L's employee at all times and not left unattended.
- I also understand that the alleged perpetrators deliberately distracted L's employee, who was, understandably, concerned about the possibility of shoplifting. This doesn't indicate L's employee was being careless or negligent, but rather that they were subject to an organised attempt to defraud and they were trying to minimise what they perceived as the risk to L.
- I've also reviewed the refund process in the terminal manual and it does not appear that processing a refund would take a significant amount of time. And, our service has seen other complaints where a skilled perpetrator is able to execute transactions swiftly.
- I've also considered that this type of fraud is relatively unusual and I wouldn't necessarily expect L to be completely alert to this risk. L says that it rarely, if ever, gives refunds by card, which also indicates that it's less likely to be aware of this particular risk.
- I understand that the risk was highlighted to L in various pieces of documentation that it was provided with. But, I haven't seen anything to suggest those warnings were particularly prominent. While a failure on L's part to read and/or understand that information (or set a refund approval limit) might have been careless, gross negligence requires that carelessness to be to a very significant degree. I don't think that can be shown here.
- GPUK point to the fact that L didn't notice the transaction for several days as evidence that they were not taking care of the terminal. This fact might indicate that they didn't notice anything unusual about the way the fraudster was using the machine or they were distracted at the time, but, again, it's not enough for me to suggest that they were grossly negligent. The fraudster may have simply been very adept at carrying out the fraud.
- So, overall, I'm not persuaded that L authorised the payment in dispute and I don't think GPUK have been able to demonstrate that it failed to adhere to the terms and conditions or Regulation 72 PSR 2017 with gross negligence or intent.
- It follows that L should be refunded in full.
- As the funds were likely to be used in the ordinary course of business, I think GPUK should also pay L 8% simple interest per annum from the date L was without the funds to the date of settlement.

My final decision

I uphold this complaint about GPUK LLP and instruct it to pay L:

- £999.99
- Any charges associated with the payment.
- 8% simple interest per annum from the date L was deprived of the funds to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask L to accept or reject my decision before 14 July 2023.

Rich Drury
Ombudsman