DRN-4474285

The complaint

A company, which I'll refer to as J, complains that PrePay Technologies Limited (trading as PPS) won't refund payments it didn't make.

Mr B, who is a director of C, brings the complaint on J's behalf.

PPS issues J's business current account and Countingup acts as its agent. For ease, I've generally referred to Countingup, although PPS is ultimately responsible for the complaint.
.

What happened

The details of this complaint are well known to both parties, so I won't repeat them again here. The facts are not in dispute, so I'll focus on giving the reasons for my decision.

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 done so, I've reached the same outcome as our investigator for these reasons:

- Countingup hasn't disputed this concerns unauthorised payments. However, it's declined to refund them under the Payment Services Regulations 2017 (PSRs) because it asserts Mr B failed with gross negligence or intent to comply with the terms of the account and keep J's personalised security details safe.

- To be clear, it's not enough to simply assert that Mr B didn't keep his security details safe or breached the terms and conditions. Instead, Countingup must show he did so with gross negligence. In other words, Mr B must have acted with a *very significant* degree of carelessness; *seriously* disregarded an *obvious* risk or fell *so far below* what a reasonable person would've done.

- To assess this, I've reflected on the circumstances of the scam. Mr B recalled he was called from someone purporting to be from Countingup about a suspicious transaction – he trusted the caller as they knew some of J's personal and sensitive information and their number matched the one on the back of J's card. Many people don't realise how fraudsters can spoof someone else's number, so I can see why Mr B believed the call was genuine.

- Countingup submit that Mr B ought to have been alarmed by the call, as it doesn't usually contact customers this way. But I wouldn't expect him to know, off the top of his head, an exhaustive list of how and in what circumstances Countingup contacts its customers. And on the whole, I don't think its implausible that Mr B believed Countingup would call him about potential fraud.

- Having confirmed that he didn't recognise a transaction, Mr B said he was asked to forward an email he received from Countingup to a specific email address they gave him – this was to prove it was him they were talking to.

- I've considered that the email says it's to register a new device and how it warns him not to forward it. Mr B says he didn't read this properly at the time – he's explained he trusted the caller and he focussed on sending it to the right email address. He added that the caller rushed him, saying they'd be able to review any other suspicious transactions afterwards.

- I've reflected on this clever misdirection, the pressure he was under, and his belief he was speaking with Countingup – something that I imagine was reinforced when emails came through from it when he'd been told to expect them. Taking this all into account, I can understand how Mr B simply followed the instructions without taking in the wider context of the email.

- In saying that, I've noted Countingup's comments about warnings in respect of authorised push payment scams. But this complaint concerns an *unauthorised card payment*. So this wasn't a warning that Mr D was required to interact with in the context of making a payment. Indeed, he was ignorant to the fact that fraudsters already had J's card details, and this was the final step in gaining access to its account. I'm also mindful that the warning wasn't especially eye-catching, particularly when viewed quickly on a phone.

- I've also considered Countingup's point that it doesn't make sense to forward an email for verification purposes. Of course, it's possible to pick holes in the logic of this with the benefit of hindsight. But I'm considering Mr B's actions in the heat of the moment when he concerned about the safety of J's money. And I note there are a variety of ways that genuine businesses verify customers – so I can see why this instruction didn't ring alarm bells at the time.

- I've finally considered the information Countingup had provided to Mr B in the past about fraud. But I don't find it persuasive to say he seriously disregarded an obvious risk, simply because he didn't pay heed to past general warnings about fraud in the immediacy of a sophisticated and elaborately planned scam.

- This isn't all to say Mr B acted perfectly reasonably – it's possible to call his actions careless. But, having considered the circumstances carefully, I'm not persuaded Countingup has shown he failed with *gross* negligence.

- I've noted Countingup also mentioned that Mr B intentionally breached the terms and conditions or failed to keep his personalised security details safe. But it's not provided any persuasive arguments or evidence to support this was a deliberate act on Mr B's part.

- It follows that I don't consider J can be fairly held liable for these unauthorised payments, in line with the PSRs. That means Countingup needs to put things right – by refunding its losses from the payments alongside 8% simple interest per year to compensate it for the time it's been out of pocket.

My final decision

For the reasons I've explained, I uphold J's complaint. PrePay Technologies Limited must:

- Pay J the total of the unauthorised payments less any amount recovered or already refunded.

- Pay 8% simple interest per year on this amount, from the date of the unauthorised payments to the date of settlement (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask J to accept or reject my decision before 21 May 2024.

Emma Szkolar
Ombudsman