DRN-4888709

The complaint

Mr P complains that Prepay Technologies Ltd (PPT) won't refund money he lost in a safe account scam.

What happened

What Mr P says:

Mr P has a business account with PPT.

On 23 January 2024, he was asked to authorise a payment of £4,099 which wasn't made by him. He suspected it was a scam, didn't authorise it and went to call PPT.

But at the same time, a call came through (with a 'no caller ID') from someone purporting to be from PPT. Mr P took the call.

The caller went through 'security checks'. He was told his account with PPT had been the subject of fraud and a fraudster had his account details. The caller instructed him to transfer the balances in his PPT accounts to a 'safe account'. He was sent a link to a website and he opened two accounts at another bank in the name of his businesses and made a number of payments to them as he was instructed to.

The payments were made between 4.41pm and 4.54pm:

Date	Payment	Amount
23 January 2024	Faster payment to Mr P's new accounts	£5,988.29
23 January 2024	Faster payment to Mr P's new accounts	£5,787.28
23 January 2024	Faster payment to Mr P's new accounts	£5,586.27
23 January 2024	Faster payment to Mr P's new accounts	£5,385.26
23 January 2024	Faster payment to Mr P's new accounts	£5,184.25
23 January 2024	Faster payment to Mr P's new accounts	£4,508.24
Total		**£32,439.59**

While he was on the phone to the caller, he got a message from PPT to say a new payee had been set up and money transferred, but as he was on the phone at the time, he says he didn't see those.

Mr P says the call was professional and genuine.

Mr P realised this was a scam and contacted PPT the next day, at just after 8am on 24

January 2024. PPT then refunded the first three payments - £17,361.84. Mr P says his business is now struggling because of the remaining loss of £15,077.75.

Mr P complained. He said PPT should refund all the money. He says:

- The Confirmation of Payee (COP) failed and so PPT should not have made the payments.
- He says that as PPT are related to NatWest, and NatWest have signed the Contingent Reimbursement Model Code (CRM Code), PPT should refund the money under the Code.
- There must have been a data leak as the scammer had all his account details.

What PPT said:

- PPT said they would refund the first three payments (£17,361.84).

- After the payees were set up, a text message was sent: "*Hang up the phone and contact us via in-app chat if you've been told to add this payee."* The message said *"We will never contact you and ask you to move your money to keep it safe."*

- When Mr P added the two new payees in the app, there were two pop up warnings about transferring money to a 'safe account'. The message asked the reason for setting up two new payees. Mr P opted for 'paying myself'. There were then a further four options including *"I've been told I need to move my money urgently to protect my account", "I've been asked to set up a new account and move money…because my account is at risk", "I've been told my money isn't safe in my …account*" and "*None of these apply to me".*

- Mr P selected "*None of these apply to me*". Had Mr P selected any of the first three options (as he should have), then there would've been a further tailored warning about fraud.

- There was a general fraud warning about scams when adding a new payee – before the other options provided.

- The payees didn't match in the COP test. There were other warning messages sent to Mr P because of this which said "*Name doesn't match account details. The name entered doesn't match the details of the person you're sending money to. Please double check the name and cancel this payment if you think it's a scam."*

- The payments weren't out of line with the normal account activity, so there wasn't a reason for PPT to intervene and stop them.

- There were general scam warnings published in PPT's app.

- There hadn't been any data leaks. It was likely Mr P's details may have been obtained through a third-party website where he had input his personal and bank details.
- PPT tried to get the money back by contacting the recipient bank, but no funds remained to be reclaimed.

- NatWest has signed up to the CRM Code, but it is a voluntary code. Mr P's account provider is 'affiliated' with NatWest but they have separate processes and procedures. It follows that PPT aren't part of the CRM Code.

Our investigation so far:

Mr P brought his complaint to us. Our investigator didn't uphold it – he said PPT had done enough to settle it by refunding £17,361.84. He said:

- The payments weren't particularly suspicious or unusual for Mr P to make. There had been similar size payments in the past for example, in November 2023 and December 2023.
- Mr P received several warning messages from PPT, and these were ignored by him.
- PPT didn't advertise they are part of the Contingent Reimbursement Model (CRM) code. And it wasn't guaranteed that the Code would provide a refund in any case.
- Even if our investigator had agreed to refund all the money – it was likely there would've been a deduction for contributory negligence – so he would have ended up with a refund of less that PPT had already paid.

Mr P didn't agree and asked for an ombudsman to look at his complaint. He said:

- He set up new payees that didn't match.
- He had never paid into the bank where the new accounts were set up.
- There were multiple payments in the scam.
- His business was suffering and he was facing a large tax bill which he can't afford to pay.

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.

I'm sorry to hear that Mr P has lost money in a cruel scam. It's not in question that he authorised and consented to the payments in this case. So although Mr P didn't intend for the money to go to a scammer, he is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story. Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider PPT should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

I need to decide whether PPT acted fairly and reasonably in its dealings with Mr P when he made the payments, or whether it should have done more than it did. I have considered the position carefully.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) provides for refunds in certain circumstances when a scam takes place. But – it doesn't apply in this case because PPT hasn't signed up to it. I considered what Mr P says about this – and PPT haven't signed up to the Code, even though NatWest have. But it's important to say that the Code doesn't provide for an automatic refund of money lost in scams such as this – claims must meet certain criteria.

The first and most important step here is – were the payments in question so unusual to have expected PPT to have stopped them and intervened.

And - in this case, I don't consider PPT acted unfairly or unreasonably in allowing the payments to be made. Whilst I understand the loss has had a big impact on Mr P, I don't consider the payments were so out of character that PPT ought reasonably to have had concerns that Mr P may be the victim of fraud. I am mindful of the fact the payments were made from a business account where larger payments aren't unusual.

I looked at Mr P's bank statements and these show similar sized payments were regularly made and in some cases, several of them were made on the same day (shown in italics) - so following a similar pattern to the scam payments in dispute:

December 2023: *£4,274, £4,615, £1,663, £3,858 (same day)*; *£10,000, £10,000* (same day)/ 6,925 / *£7,500, £10,000, £7,073 (same day).*

November 2023: £3,500, £7,298 / *£10,000, £10,000, £5,000* (same day)/ *£10,000, £4,256 (same day).*

October 2023: *£9,000, £10,000, £8,000 (same day) /* £6,840, £3,576, £3,160 / *£10,000, £3,000, £3,600, £7,000 (same day).*

So - none of the disputed payments were particularly different in value as Mr P had made payments of similar value in the months before the scam. And whilst all the disputed payments were made on the same day, this wasn't unusual either compared to Mr P's normal account activity.

And also - there's a balance to be made: PPT has certain duties to be alert to fraud and scams and to act in their customers' best interests, but they can't be involved in every transaction as this would cause unnecessary disruption to legitimate payments. In this case, I think PPT acted reasonably in processing the payments.

Mr P says that PPT shouldn't have put the payments through because the COP test failed – but the purpose of the COP check is for customers to consider whether they are sending payments to the correct and intended payee – it doesn't mean that a firm must refuse to put payments through. And here, because the COP check failed, PPT sent to Mr P the relevant warnings about what he was doing – which is what we would have expected them to do.

Therefore, in all honesty, I think PPT have been very reasonable in refunding the first three payments to Mr P. Had they not done so, I'm persuaded that it would be unlikely that this service would've gone as far as PPT did – for the reasons I've given.

I noted that Mr P didn't take any action when he was sent the various warnings by PPT – but I've not gone on to consider those and what that means for this complaint. What they suggest is that Mr P contributed to his losses and therefore any refund our service may award would be reduced accordingly. And as this decision is that no further refund is needed, I don't need to consider a deduction.

Recovery of Funds:

We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether PPT took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money. I can see PPT contacted the bank at 10.25am on 24 January 2024 – within two hours of Mr P contacting PPT. So – that was within a reasonable timescale. But unfortunately, no funds remained. I'm not surprised at that – as it is common in such scams that funds are removed immediately by the fraudsters.

Mr P has lost a lot of money. He's explained why the money was important to his business, and the impact the losses have had. I was sorry to learn of his circumstances. He will therefore be disappointed by my decision, but I'm not going to ask PPT to do anything more here than they already have.

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr P to accept or reject my decision before 29 November 2024.

Martin Lord
Ombudsman