DRN-6318346

The complaint

Mr F complains that PSI-Pay Ltd ("PSI-Pay") won't refund the money he lost to a scam.

Mr F opened an account with Pockit Limited. The Pockit Card is issued by PSI-Pay Ltd. For simplicity, I'll generally refer to Pockit throughout this decision.

What happened

In summary, on 15 November 2024, Mr F was called by someone (a scammer) claiming to be from his personal bank's ("Bank N") fraud department. He was led to believe his account with Bank N had been compromised and frozen. As Mr F was abroad at the time, spreading his mother's ashes, a call back was arranged for a few days later.

Mr F was back in the UK on 16 November 2024. On 18 November 2024, the scammer called again and Mr F was told that, as a temporary measure, he could open new accounts with Pockit and another payment service provider ("R") to cover direct debits and standing orders. Mr F has said this was a concern for him with bills and mortgage payments due.

A new Pockit account was opened by Mr F on 19 November 2024 while the scammer talked him through the process. Mr F then made two payments from Bank N into his new Pockit account. Mr F accepts that, in that call, he shared security credentials for his Pockit account and that he may have also shared the codes he received. But he says he did so believing he was speaking to someone from Bank N's fraud team who was helping with setting things up.

He says he became suspicious later that day when he saw that two payments had been made from Pockit to a crypto-platform ("M") and that because these payments were made without his knowledge they should be treated as unauthorised and refunded.

Date	Time	Merchant	Method	Amount
19-Nov-24	14:01		*Credit into Pockit*	*£950*
19-Nov-24	14:02	M crypto-platform	Card payment - online	£945
19-Nov-24	15:00		*Credit into Pockit*	*£2,050*
19-Nov-24	15:20	M crypto-platform	ApplePay - online	£2,050
19-Nov-24	15:53		*Failed credit into Pockit*	*£2,000*

Mr F says he contacted Bank N on 19 November 2024 to report what had happened. He was told to raise a dispute with Pockit, which he did the following day. In March 2025, Pockit said it wouldn't be refunding the disputed payments, so Mr F referred his complaint to our Service. Our Investigator considered it and upheld it.

Regarding the £945 payment, the Investigator considered it unauthorised. He concluded that while Mr F likely shared his card details and the SMS one-time passcode ("OTP") used to authenticate the transaction, he did so because he genuinely believed he was speaking to Bank N's fraud team and didn't realise a payment would be made. For the £2,050 payment, the Investigator found that the scammer had used Mr F's security credentials to add the Pockit app to their own device and set up an ApplePay token. Because Mr F didn't share his details for the purpose of making a payment, and wasn't involved in setting up ApplePay, he

considered this payment unauthorised as well. As he didn't think Mr F had acted with intent or with gross negligence, he said Pockit should refund both payments.

Mr F accepted this outcome. Pockit said that the transactions were authorised. The first was authenticated via a OTP sent to Mr F's registered number. For the second, the scammer could only have set up the app on their device with full verification, including entering Mr F's password, Mr F approving a "magic-link" email, and Mr F sharing an OTP. Pockit said that adding ApplePay on the scammer's device would have required a further OTP sent to Mr F's phone. It also said Mr F didn't attempt to verify with Bank N if his account had been frozen, Bank N provided fraud warnings, the OTP for the first payment would have shown M as the merchant, and his repeated sharing of security details all amounted to gross negligence.

Provisional decision

I issued my provisional decision on this case. I set out the background as above and explained why, on the evidence, I wasn't minded to uphold it. I provided these reasons.

Can Pockit fairly treat the payments as authorised?

Under the Payment Services Regulations 2017 ("PSRs"), Mr F is responsible for payments he authorised. With limited exceptions, Pockit is responsible for unauthorised ones. A payment is usually considered authorised when the customer makes it themselves. But it can also be treated as authorised if the customer gives permission for someone else to make it on their behalf or they instruct their payment service provider to proceed.

I accept Mr F genuinely believed he was speaking to Bank N's fraud team. I also accept the scammer probably initiated the payments from Pockit by entering Mr F's card details on M's website. So I don't think Mr F made the payments himself. What is less clear is whether he gave permission for someone else to make them. Mr F denies doing so and his account of events suggests he believed he was only moving funds into Pockit to cover bills while issues with his Bank N account (which Mr F thought was under "embargo") were being resolved.

However, several actions taken by Mr F were, on the face of it, consistent with someone allowing another person to make payments, even if the reasons are not understood. The technical evidence provided by Pockit for 19 November 2024 shows the following key events. At 13:26, the app was added to Mr F's Android device and Google Pay was set up on that device soon after. At 13:31 the card details were viewed. Mr F doesn't appear to dispute sharing these with the scammer. At 14:02, the first disputed payment was made, authenticated using an SMS OTP sent to Mr F's registered number. The text would have read: "xxxx is the One Time Password for purchase of GBP XXX at [Merchant] with card ending xxxx. Please use the One time Password to complete the transaction".

In between 14:05 and 15:18 and again from 15:55, there were multiple logins into the app from Mr F's device. At 14:11 Mr F appears to have submitted a request to increase account limits. At 15:11, the Pockit app was added to a new device (the scammer's iOS). Although the scammer was provided with Mr F's login details, Mr F would still have needed to approve the addition of a new device via a "magic link" email and a further SMS "verification code". At 15:20, Mr F's card was added to the scammer's device which Pockit says would again have required both "magic link" email approval and a code sent to Mr F registered details.

At 15:20, the second payment was made via ApplePay on the scammer's device. And at 15:53 another incoming payment of £2,000 from Bank N was blocked. This triggered Pockit's "source of funds" check and a request for Mr F to provide ID, proof of address, a selfie, and a reason for account use which was given as "daily spending and holidays and investments".

When our Investigator asked Mr F why he shared his security information, he said he could not recall sharing an OTP, but accepted he may have done so, along with "activation codes", because he had been taken in by the scam. He explained that he shared his login details because he believed this was necessary due to problems transferring funds from Bank N to R. He said he thought it would be quicker if the caller (he believed was from Bank N) had this information for operational reasons and to facilitate something akin to an account switch while the caller supposedly liaised with Pockit's fraud team without Mr F's involvement.

As part of my investigation, I provided Mr F with an example of the SMS OTP required to approve the first payment and asked again what he recalled about sharing it with the scammer. I also asked about the "magic link" emails he would have needed to approve to allow the scammer to add the app on their device. I referred to the multiple logins from Mr F's own device between the first and second payments and asked what he recalled about his account balance reducing during that period. I further asked why he transferred funds from Bank N into Pockit in smaller amounts rather than as a single transfer. And why he shared his Pockit security information with someone claiming to be from Bank N when there appeared to have been no difficulty opening or crediting the Pockit account itself.

Mr F was unable to provide much additional detail, which is understandable given the passage of time. Even so, it remains the case that he took a number of steps and shared a significant amount of information. There remain gaps in his explanations for those actions. Based on the evidence, I'm not persuaded that it's more likely than not that Mr F took the steps shown without any understanding that he was enabling a third party to transact on the account, even if he did not appreciate that money would be sent to a particular merchant.

For example, Mr F says he believed his Bank N account had been frozen and that funds sent to Pockit were intended to cover bills. There does not appear to have been an urgency suggesting his funds were at immediate risk, particularly as a call-back had been arranged for days later. Even accepting Mr F believed he was dealing with a trusted source, it's unclear why he would not have read or questioned the content of the SMS OTP for the first payment, which explicitly referred to authorising a payment he says he did not expect.

Evidence from Bank N and R shows that attempts to transfer money from Bank N to R took place on 20 November 2024, the day after the payments into (and from) Pockit. I again realise that recollections fade. However, this does not align with Mr F's explanation that he shared his Pockit account details because of earlier difficulties transferring funds from Bank N to R. It's difficult to reconcile those later transfer attempts with Mr F's account that, by this point, he had already become suspicious after seeing unexpected payments from Pockit to M. Given that the audit logs also show Mr F accessing the app on his device between the disputed payments and again afterwards, during which time he would likely have seen the account balance, it's not clear why Mr F wouldn't have reported that matter sooner than he did if the transactions were again unexpected.

I recognise Mr F was the victim of a scam and deceived by a convincing fraudster. I don't imagine he would have gone along with what happened had he understood the risk of losing his money. However, for the reasons above, I'm not persuaded that the payments should fairly be treated as unauthorised. Even if I were to find the payments were unauthorised, I would still need to consider whether Mr F failed with intent or gross negligence (the terms used in the PSRs) to keep his personalised security details safe – either of which would entitle Pockit to hold Mr F liable for the transactions despite them being unauthorised.

As set out above, there does not appear to have been an immediate risk to Mr F's funds. He appears to have shared a OTP that explicitly referred to a specific payment being made. Mr F also shared his Pockit card details and account security information (with someone he believed to be from Bank N) but it's not sufficiently clear to me that he was provided with a

particularly plausible explanation as to why all those details were required by them. There was a gap between calls and, as Pockit has highlighted, Mr F could arguably have taken further steps to verify the caller's identity, for example by contacting Bank N directly. Bank N has also provided evidence of the fraud warnings that would have been displayed when the transfers into Pockit were made. Based on the likely payment reason selected, Mr F would likely have been shown a warning stating: "Banks, the Police, HMRC or any other trusted organisation will never call and ask you to move money to another account – this is a scam".

I'm mindful of what Mr F has shared with us about his condition and the difficult personal circumstances he was facing at the time. However, on the information available and taking all the above factors into account, I would be minded to conclude that Pockit can hold Mr F liable for failing with intent or gross negligence in keeping his security credentials safe, if the payments were to be treated as unauthorised.

Should Pockit have done more to prevent the scam?

In broad terms, a firm is expected to process payments and withdrawals that a customer has authorised. While there are some situations where additional checks are appropriate, the payments in this case, though not insignificant, would not have appeared as particularly concerning in value. I'm also mindful that the account was newly opened, meaning Pockit had limited information on which to assess a possible scam risk.

In the circumstances, I don't consider it unreasonable that Pockit didn't step in on concerns that Mr F was at a heightened risk of fraud when the disputed payments came about.

Should Pockit have done more to recover the money?

As the disputed transactions were card payments, a potential recovery route for Pockit was the chargeback scheme – operated by the scheme provider to resolve disputes between customers and merchants, subject to the scheme rules. I'm satisfied it's unlikely such a claim would have succeeded here as it is not in question that the merchant, M, provided its services as intended, albeit to a scammer and not for Mr F's benefit.

I realise this will be disappointing for Mr F. I'm very sorry he was scammed and for the impact this had on him at an already difficult time. I've thought carefully about what I think is a fair and reasonable outcome and the matter is finely balanced. However, for the reasons set out above, I'm not persuaded I can hold Pockit liable for Mr F's losses in this case.

Responses to provisional decision

I invited further comments and evidence from both parties. I explained that, unless any new information changed my view, my final decision was likely to be in line with my provisional conclusions. Pockit accepted the provisional decision.

Mr F responded saying he thought the provisional decision was grossly unfair considering that the payments to M were made using a different number and device. He said that Pockit should have had facial recognition system in place to prevent what happened.

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'm not persuaded to depart from the conclusions reached in my provisional decision, which is copied above and forms part of this final decision.

In my provisional decision, I explained that the payments to M were made by card using details that Mr F accepts he shared with the scammer. The first was authenticated using a one-time passcode, which clearly stated it related to a payment, and was sent to Mr F's phone number. The second was made after Mr F shared additional security information, enabling the scammer to add the Pockit app to their own device and set up ApplePay.

I accept that Mr F shared his information because he genuinely believed he was speaking to Bank N, having been told that fraud had been detected on his account. I've also considered his suggestion that facial recognition would have prevented his losses. However, I still can't overlook that Mr F took several steps that enabled the scammer to complete the payments.

In the absence of any further explanation for why these steps were taken, or for some of the significant discrepancies I referred to between the technical evidence and aspects of Mr F's recollections, I don't consider it fair to conclude that the payments were likely unauthorised. For similar reasons, even if I were to say that the payments were unauthorised, it would be difficult, on the evidence, to conclude that Mr F could not still be held liable for failing with intent or gross negligence to keep his security information safe.

This is not a decision I've reached lightly. I'm again mindful that Mr F was the victim of a scam and that these events occurred during an already difficult time for him. However, no new material evidence or arguments have been provided that would lead me to change the outcome reached in my provisional decision, for the reasons previously explained.

My final decision

For the reasons given, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 25 May 2026.

Thomas Cardia
Ombudsman