

The complaint

A limited company which I'll call 'P' complains that ANNA Limited won't refund the money it says it lost as the result of a scam.

PayrNet Limited operate P's account on ANNA Limited's behalf, so I'll only refer to PayrNet throughout the decision.

The complaint is brought on P's behalf by its director, Mr P.

What happened

Both parties are aware of the circumstances of the complaint, so I won't repeat them all here. But briefly, Mr P says on 26 March 2024, he received a call from someone he believed to be from PayrNet. The caller said they'd identified fraud on P's account and that authentication changes were required. Mr P says that he was told to apply the required dual authorisation, he needed to share the One Time Passcode (OTP) which would be received shortly.

An OTP was received from the real PayrNet asking for a new device to be added to P's account. Mr P says he gave the OTP to the caller and shortly after, he received messages saying additional contact numbers had been added to P's account. Mr P said he explained his frustration with the PayrNet app and was told by the caller that all his business accounts could be linked together. He was happy with this and believed his accounts were now safe and the call ended. Mr P says he received a call back later in the day to say that all his accounts had been linked under a master account and he would receive communication about other devices being added, which was the system trying to confuse the person who had committed fraud.

On 28 March 2024, one of Mr P's other companies received a large credit from a loan into its account with PayrNet. Mr P then made a series of six transfers moving the balance of the credit from this PayrNet account to his personal account, which was held with a bank I'll refer to as 'W'.

On 3 April 2024, Mr P says he received a further call from PayrNet whilst he was abroad. The caller said they were calling from the Financial Ombudsman Service's number. Mr P says he checked the number was correct and reassured he asked them to call him back on WhatsApp. Mr P said he received a call via WhatsApp and checked the number was correct from PayrNet. The caller said that there had been fraud on P's account, and someone had tried to apply for a loan in P's name and the wanted to check if this was correct as PayrNet don't offer loans.

The caller also said W had contacted it to say that Mr P's personal account was also at risk. They said Mr P should return the funds that he'd recently moved from his businesses account with PayrNet to his account with W, so that these could be protected, as funds held with W weren't protected by the Financial Service Compensation Scheme (FSCS). Mr P says he was told by the caller that the funds in P's account would be moved to the new safe account, and that he would receive a text message with an OTP for the payments to take

place. He says he was told that each of the individual payments which would be made would end in £0.08 so he'd be able to identify them. Mr P says he then received a message from PayrNet saying that a payment for £1,993.08 was being made, along with an OTP, which he then shared this with the caller. The payment was then released, followed by two additional payments.

Around the same time, Mr P says he received a text from a number he'd previously received messages from W from, so he was reassured. The caller said that W would be calling Mr P shortly after their call had ended to assist him. Shortly after, Mr P received a call from who he believed was W. He was again told that he should transfer the funds from his personal account to P's PayrNet account for protection. He says he was told the funds would be transferred into individual safe accounts and each of these accounts would hold no more than £85,000 so that they would be protected by the FSCS. Mr P says that he then made eleven payments totalling £430,000 from his account with W to PayrNet

Mr P says that he was told by the caller to transfer funds from his other business accounts to P's account with PayrNet so they could be moved to individual accounts holding a maximum of £85,000. However, as it was late in the evening he said he would do this the following day. Mr P says the next day he transferred the remainder of the funds and tried to text the number he held for the caller, but it wouldn't go through. He then logged into his PayrNet app and saw that all the funds had been removed in the following transactions:

Date	Payee	Amount	Transaction completed/Not completed
03-Apr-24	M	£1,993.08	Completed
03-Apr-24	M	£9,000.08	Completed
03-Apr-24	M	£5,055.08	Completed
03-Apr-24	M	£25,000.08	Completed
03-Apr-24	M	£15,000.08	Completed
03-Apr-24	D	£25,000.08	Completed
03-Apr-24	K	£25,000.08	Completed
03-Apr-24	D	£20,000.08	Not completed
03-Apr-24	B	£40,000.08	Completed
03-Apr-24	P	£30,000.08	Completed
03-Apr-24	BC	£25,000.08	Completed
03-Apr-24	J	£30,000.08	Completed
03-Apr-24	S	£30,000.08	Completed
03-Apr-24	G	£25,000.08	Completed
03-Apr-24	BM	£30,000.08	Completed
03-Apr-24	SC	£40,000.08	Completed
03-Apr-24	P	£40,000.08	Completed
03-Apr-24	I	£30,000.08	Completed
03-Apr-24	A	£25,000.08	Completed
03-Apr-24	SS	£30,000.08	Completed
03-Apr-24	JA	£30,000.08	Not completed
03-Apr-24	T	£40,000.08	Completed
03-Apr-24	SG	£30,000.08	Completed
03-Apr-24	CK	£30,000.08	Completed
03-Apr-24	MM	£40,000.08	Completed

03-Apr-24	PC	£13,105.08	Completed
		£664,155.00	

In total, 26 transfers totalling £664,155 were attempted from P's account. However, only 24 actually completed as two payments for £20,000.08 and £30,000.08 were returned immediately to P's account, meaning £614,154.84 actually debited P's account. Mr P said he contacted PayrNet and asked it to return the funds as he hadn't authorised the payments. PayrNet declined to refund P and when he didn't receive a satisfactory response to P's complaint, Mr P asked our service to look into it.

PayrNet told our service that it didn't think P met the eligibility criteria to bring its complaint to our service as it was part of a group of companies which was too large to be a micro-enterprise or small business. So, it didn't think our service had the jurisdiction to consider P's complaint. However, it said notwithstanding that, it wouldn't be reimbursing P as it thought Mr P had shared his log-in information with a third-party which breached the terms and conditions of the account. It also said it had acted promptly when it was notified of the fraud and taken all reasonable steps to recover P's funds, of which £66,095.02 had been recovered.

Our investigator thought that P met the eligibility criteria for a small business and therefore our service could consider its complaint. However, he didn't recommend the complaint be upheld. He said that after the complaint had been brought to our service, Mr P had changed his mind about the payments being authorised and what he'd known about the transactions. The investigator noted that Mr P's version of events was inconsistent throughout, so it was difficult to say for sure what had happened. But he thought by telling PayrNet that he was aware of the transfers being made to a safe account, he'd made a representation to PayrNet that the payments were being made on his behalf.

The investigator thought that even if that wasn't the case and Mr P hadn't authorised the payments, it was reasonable to PayrNet to decline to reimburse him as he hadn't kept his security information safe. The investigator said he'd considered if PayrNet had done enough to prevent P's loss, and he didn't think it had done anything wrong. He said the account activity wasn't unusual for P's accounts, but even if PayrNet had intervened, as Mr P had said he was aware of the activity, this wouldn't have changed if PayrNet had contacted him.

Mr P didn't agree and asked for an ombudsman to review his complaint. In summary he said:

- PayrNet should have provided an OTP for each payment and a selfie, but none had been requested.
- He hadn't authorised the payments as he was deceived into thinking the money was going to safe accounts, so he hadn't consented or authorised the payments.
- It was for PayrNet to prove he had authorised the payments but all it could show was that he'd given an OTP, so this also wasn't gross negligence.
- PayrNet had failed in its duty of care by allowing £600,000 to leave P's account without additional checks.

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 sorry to disappoint P's director but I'm not upholding the complaint, so I won't be asking PayrNet to refund P's loss as a result of the purported scam.

The regulations relevant to this case are the Payment Services Regulations (the PSRs). These explain that a payment can only be authorised if the payer has consented to it. This is important because, generally speaking, account holders will be liable for payments they've authorised, and banks will be liable for unauthorised payments. I've taken this into account when considering what's fair and reasonable in the circumstances of this complaint. However, that's not the end of the story, because I still need to take other things into account, such as the actions of both the account holder and the account provider, any account terms and conditions, amongst other things.

With that in mind I do just want to clarify some information for Mr P. Firstly, he's said that he doesn't think that PayrNet have acted in line with the Contingent Reimbursement Model (CRM) Code. However, that was a voluntary code which PayrNet weren't signed up to, and it also wouldn't be applicable in this case because P doesn't meet the eligibility criteria for the Code as Mr P has already told us that P would be a small business based on the accounting information for his group of companies. He's also mentioned numerous decisions regarding how authorisation and the use of OTPs should be considered, along with the legal precedent for gross negligence. However, each case is reviewed on its own merits, and my role is to consider the circumstances and evidence provided for this case alone.

Generally, the first thing for me to consider here is whether or not it was fair for PayrNet to say these payments were authorised by Mr P. And I think it was. I recognise that Mr P says he didn't authorise the payments and he was deceived that they were going to safe accounts. However, based on the evidence available I'm not persuaded by Mr P's testimony.

I say that because since the complaint was brought to our service, Mr P has changed his version of events on several occasions and the evidence provided is inconsistent with what Mr P has claimed. For example, Mr P said that it was only in the morning of 4 April 2024, he realised that there was no money in P's account, and he'd been scammed. However, he also subsequently said that he was aware the transactions were happening but thought the funds were being moved to safe accounts and that he wasn't aware of the payees – which is also inconsistent with what Mr P told PayrNet.

On that occasion, Mr P said that he'd seen the new payee's and payments being made. Mr P also said that his finance manager messaged him about the first payment which was made from P's account, and he wasn't concerned as he said was on the phone to the bank which was transferring the money to a new account. So, based on what I've seen I think it was reasonable for PayrNet not to reimburse P as the payments from its account were authorised.

However, even if I am wrong about that and Mr P didn't authorise the payments, I think it was reasonable for PayrNet to decline to reimburse P for these transactions. PayrNet's terms say that:

"You are responsible for the use of your Account and any Cards issued for your Account. You must ensure that all the users of your Account including any Cardholders and Account Users understand and comply with this agreement"

They also say:

You will be liable for unauthorised transactions that arise from the use of a lost or stolen or otherwise misappropriated Card or Account security information or the device used to access the Account if you or any Cardholder fails to:

- (a) keep the card/and or security features of the Card, Account, Account-security information or device used to access the Account safe, or*
- (b) notify us [...] that the Account security information or your device have been otherwise access or misappropriated".*

In this case, it's not disputed by either party that Mr P knowingly shared the OTP to allow a third-party device to be added to his account, so I think it's reasonable to say that he didn't keep the security information used to access his account safe. I've seen evidence from PayrNet that the device which Mr P allowed to access P's account using this OTP was the one used to make the disputed transactions from P's account. So, I think it would be reasonable for PayrNet to decline to refund P based on the account terms.

I recognise that Mr P says he was concerned that his business accounts were being used fraudulently, and that he was reassured by the caller, so he shared the OTP. I also acknowledge that he says the warnings presented by PayrNet weren't sufficient. However, PayrNet has provided evidence of previous warnings which said that PayrNet would always arrange any calls within the app before these took place. Mr P also recalled on the call with PayrNet on 4 April 2024 that the caller said they were going to merge all his business accounts into one new security system. However, I can see that Mr P was told by PayrNet shortly after he'd shared the OTP that it was simply not possible for the accounts to be grouped together. He was also reminded a few days later on an in-app chat that PayrNet was an app-based entity and all contact was initiated through the app. So, I think there were other prompts received by Mr P around the time of the transactions which ought reasonably to have prompted him that something wasn't quite right.

Mr P says that our investigators opinion was unfair as it didn't fully consider the actions of PayrNet when the transactions were made. He says PayrNet should have done more checks and therefore it should be held liable for P's loss. But I don't agree. I have received information from PayrNet regarding its decision not to refund P's loss which it claims was the result of a scam. I recognise that Mr P may wish to know more about this evidence, however DISP rule 3.5.9(R) allows me to accept sensitive evidence in confidence – for example if it contains information about third parties or security procedures. But I see that it is appropriate here that this evidence remain confidential, therefore I won't be commenting further on the specific evidence it has provided regarding this point. However, I'd like to reassure Mr P that I have seen the information from the bank about its decision, and I'm satisfied by the information it provided.

Therefore, upon reviewing this evidence, along with the information and evidence provided by Mr P, and other information of which I am aware, I'm satisfied that it would be inappropriate for me to award redress to P. This means that in the circumstances of this case, it is irrelevant whether PayrNet could have done more because I wouldn't see it as appropriate to award redress in this case. I recognise that this will be disappointing for Mr P, and I acknowledge he says the impact of these transactions has been financially impacted P. But based on the information available to me I don't think PayrNet has treated P unfairly or behaved unreasonably. Therefore, I won't be asking it to do anything more.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask P to accept or reject my decision before 24 December 2025.

Jenny Lomax
Ombudsman