DRN-5716177

The complaint

A company, which I'll refer to as G, complains that PayrNet Limited ("ANNA Money") is holding it liable for unauthorised payments. Mr and Mrs C, who are directors of G, bring this complaint on G's behalf.

What happened

On 25 November 2023, Mr C received a call from a scammer posing as ANNA Money's fraud department. The caller claimed someone was trying to access G's account. Mr C says they were calling from a number which he looked up and appeared to relate to ANNA Money and they also knew information about the account use – so he trusted the caller.

As Mr C was driving, the caller directed him to pull over so they could take steps to prevent funds leaving G's account. He says he was directed to delete his ANNA Money app and then re-download it along with another app, and to then log back in using his normal password but what appeared to be an ANNA Money email address, However, this email address doesn't actually belong to ANNA Money nor was it added to the account.

I can see that a new device was then added to G's account, seemingly using a code sent to Mr C. Using the new device, the scammer tried to make a payment to a new payee. But when ANNA Money asked for an invoice/documentation in order to process this, the scammer then asked to cancel the transaction and add a new cardholder instead.

G's card was then blocked. Mr C has confirmed he did this as the scammers were telling him that fraud was being attempted. But it was unblocked shortly after. Another new device was then set up on G's account, again using a code sent to Mr C. Using the second new device, the scammer added it to their Apple Pay wallet – which required knowledge of a further code sent to Mr C.

Adding the card to Apple Pay prompted an automatic block by ANNA Money. But the audit trail shows the scammer removed this in-app, using the second new device. Three card payments – for £5,000, £5,796 and £8,397 respectively – were then paid to "S", a genuine merchant, using the newly set up Apple Pay token.

After the scam call ended, Mr C called ANNA Money and it was established that he had been scammed. During this call he said he thought he had shared a code with the scammer, saying he was told the caller (who he thought was ANNA Money) needed it to help, and that he was panicked about the possibility of money being taken.

ANNA Money said it couldn't recall the payments and that it wasn't liable to refund G as Mr C had compromised the account security by sharing security credentials. Unhappy with this outcome, Mr and Mrs C (on behalf of G) referred the matter to our service.

Our investigator upheld the complaint and recommended ANNA Money should refund G in full for the payments (plus interest). She concluded the payments were unauthorised and that Mr C hadn't failed with intent or gross negligence to keep his security details safe.

ANNA Money has appealed the investigator's outcome. In summary, it says Mr C shared codes with the scammers, who he chose to listen to while ignoring the warnings in the messages it sent. And when he reported the scam, he admitted he was distracted and not concentrating when he got the scam call – and also that he hadn't read ANNA Money's full terms and conditions, and that his email had been hacked previously. He also mentioned his sister had fallen victim to a scam, so he should have been more aware of the risks.

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 decided to uphold it. I'll explain why.

The relevant law here is the Payment Services Regulations 2017 (PSRs). Broadly, in line with the PSRs, the starting position is that G isn't liable for payments it didn't authorise – unless it failed with intent or gross negligence to comply with the terms of the account or keep its personalised security details safe.

Here, it seems to be accepted the payments weren't made or by Mr C (or anyone authorised to act for him or G) but by the scammers. However, I've looked at the steps involved in setting up the payments.

It's clear the scammers got access to G's account. It's also clear they took a lot of the steps to initiate/make these payments, using the new devices added to the card. For example it's clear from the audit information that it was the scammers using these devices, rather than Mr C, who tried to set up a transfer and a new cardholder, as well as unblocking the card once Apple Pay was set up.

Mr C was prompted to enter his password/login details for G's account after being prompted to download apps which it appears granted some form of remote screensharing access. So, that explains how the scammers obtained some of the security information needed to set up these payments without Mr C directly sharing them. However, to grant the new devices access to the account and to ultimately confirm G's card being added to the Apple Pay wallet, the scammers would also have needed access to codes he was sent.

Mr C did admit sharing a code when he first reported the scam, but it's unclear if he shared all of the codes needed to set up the new devices and the Apple Pay token. It's plausible he didn't, given the use of remote screensharing software during the scam which may have allowed the scammers to see some of the messages. But as I do think it's clear Mr C shared at least one code, I've considered whether he was effectively delegating the scammers' authority to make payments on G's behalf.

When Mr C spoke to ANNA Money immediately after the scam call, he said he shared the code(s) as he thought and was told the caller – who he believed to be from ANNA Money – needed this to gain permission/access to protect his account. I don't think he was granting them authority to make payments. This is further supported by Mr C's actions in blocking his card after being told fraud was being attempted – showing he was acting to prevent payments being taken. At the time he accessed the account, no payments had been taken by the scammers – so he wouldn't have known they could get back in to unblock the card and set up Apple Pay.

Overall, Mr C's explanation and actions consistently demonstrate he thought the caller was from ANNA Money and that he was following their instructions to secure G's account. In that context, I don't think the steps he took, or his understanding of the matter, amount to him consenting to a third party making payments on G's behalf.

I therefore don't think ANNA Money can fairly treat these payments as authorised. It seems to me it accepts this – but thinks G should be held liable due to Mr C's negligence. As touched on above, the PSRs would allow ANNA Money to hold G liable if the payments were made due to Mr C (on G's behalf) failing with intent or gross negligence to comply with certain obligations, such as keeping their security information safe.

I consider it clear Mr C didn't intentionally fail to keep his details safe. He only shared them with who he thought was ANNA Money, due to being tricked into thinking this would help protect his account. I'm also not persuaded ANNA Money has shown Mr C was grossly negligent in sharing the code(s). The bar for this is high; to apply this, I'd expect ANNA Money to show Mr C showed a very significant degree of carelessness beyond what a reasonable person in his situation would have done.

It's clear Mr C was being socially engineered and tricked by the scammers, using sophisticated techniques such as spoofing a genuine ANNA Money phone number. I also consider Mr C took reasonable action in looking this up to check. He says they also knew about genuine transactions made on G's account. So, I can see why he was convinced he was speaking to ANNA Money and therefore trusted the caller.

The premise of the scam centred around Mr C being put under pressure and thinking he had to act quickly and follow the caller's instructions to protect his account. As the investigator pointed out, ANNA Money sent Mr C a code to read out when he called to report the scam – so the premise of sharing a code wouldn't reasonably have seemed that unusual or concerning.

Mr C has also explained the caller told him they would be sending him a code which he needed to share – so had primed him to expect this. In the circumstances, I don't consider it grossly negligent he overlooked the information and warnings shown in the texts – and didn't realise the risk in sharing them. I think that is also supported by the actions he took to protect his account, such as blocking his card.

ANNA Money says Mr C admits he was driving and was distracted when the scam call came through. But I think being distracted falls far short of the bar for gross negligence. Mr C did also pull over to then deal with the call, to negate some of the distractions within his control.

I don't think the fact Mr C knew his sister had been scammed previously holds much relevance either. ANNA Money hasn't shown the circumstances were so similar that it was significantly remiss of him not to realise in the moment that he was also falling victim to a scam.

ANNA Money also mentions Mr C telling them his emails had been hacked previously – and that he hadn't read the account terms. I struggle to see how having some awareness of email hacking means Mr C should have realised he was being scammed or known not to share the codes. And even if Mr C had been more familiar with the account terms, I can't see it would have been grossly negligent for him not to recall them fully here under the stress of the scam– and/or not to connect them to what was going on and identify that he shouldn't share the code(s). So I don't consider these points persuasive evidence of gross negligence.

Overall, I don't think Mr C seriously disregarded an obvious risk by sharing any security information. Rather, I think he didn't foresee this risk due to the tactics of the scammers and the circumstances he was in. While I appreciate Mr C's actions arguably exhibit *some* carelessness, all of this must be considered in context. He was put under pressure to follow the instructions of the caller, who he believed he had verified were from ANNA Money.

Given all of this, I don't think Mr C's actions can reasonably be deemed to meet the bar of gross negligence. That means, under the PSRs, I consider ANNA Money liable for the payments taken during the scam.

Putting things right

PayrNet Limited should refund G in full for the three payments taken during the scam (less any funds already recovered or refunded). It should also pay 8% simple interest per year on top of this amount, running from the date of the payments to the date of settlement. This is to compensate G for the loss of use of these funds.

If PayrNet Limited considers that it's required by HM Revenue & Customs to deduct tax from that interest, it should tell Mr and Mrs C (on behalf of G) how much it's taken off. It should also give them a tax deduction certificate if they ask for one, so they can reclaim the tax from HM Revenue & Customs if appropriate.

My final decision

For the reasons given above, my final decision is that I uphold this complaint and direct PayrNet Limited to put things right in the way I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask G to accept or reject my decision before 9 January 2026.

Rachel Loughlin
Ombudsman