DRN-6059788

The complaint

M Ltd complains that PayrNet Limited won't reimburse money it lost to a scam.

What happened

M Ltd is represented by its director, Mr B. This complaint concerns an Absolutely No Nonsense Admin ("ANNA") account. ANNA are a distributor of PayrNet Limited.

The background to this complaint has been set out in considerable detail over two different assessments, so I won't repeat it all here. In brief summary:

- Mr B received a call from someone claiming to be ANNA.
- He was told that payments had been attempted on his account. Mr B said he had no knowledge of these payments.
- He was instructed to move money to a new account to keep it safe.
- He authorised 13 debit card payments to a money remittance business and one faster payment to another person's bank account.

A table of those payments, and other activity, is set out below.

Payment number / event	Type of payment	Time	Amount
Incoming call from unknown number		17:55	
Incoming call from "spoofed" Financial Ombudsman Service number		18:32	
An attempted payment is cancelled and a virtual debit card is set up		18:43	
Payment 1	Card payment	18:51	£3,800.00
Payment 2	Card payment	18:52	£3,799.00
Payment 3	Card payment	18:54	£3,798.00
Payment 4	Card payment	18:55	£3,797.00
Payment 5	Card payment	18:56	£3,796.00
Payment 6	Card payment	18:57	£3,795.00
Incoming call from unknown number		18:57	
Payment 7	Card payment	18:59	£3,794.00
Payment 8	Card payment	19:03	£3,793.00
Payment 9	Card payment	19:05	£3,792.00
Payment 10	Card payment	19:06	£3,791.00

Payment 11	Card payment	19:08	£3,790.00
Payment 12	Card payment	19:09	£3,789.00
"Spoofed text message" received by Mr B		19:18	
Payment 13	Card payment	19:25	£3,788.00
Mr B contracts ANNA over its in-app messaging service with the message "contact number"		19:36	
Mr B makes an outgoing call to the Financial Ombudsman Service.		19:38	
Mr B makes an outgoing call to the Financial Ombudsman Service.		19:41	
Mr B contracts ANNA over its in-app messaging service with the message "help"		19:42	
Mr B emails ANNA saying that someone had taken money from his account.		19:50	
Payment 14	Faster payment	19:52	£9,000
		Total loss	£58,322

- The investigator concluded that ANNA should have intervened and prevented the scam from the third payment that was attempted and, until the last payment, M Ltd should be fully reimbursed. In relation to the final payment, they thought that responsibility for it should be shared between M Ltd and ANNA
- They concluded that, in relation to the final payment, ANNA could fairly rely on the Consumer Standard of Caution Exception ("the Exception") under the FPS and CHAPS Reimbursement Rules ("the Reimbursement Rules") to decline reimbursement on the basis that Mr B had failed to have regard to ANNA's interventions with gross negligence.
- Mr B, on behalf of M Ltd, accepted our investigator's view. ANNA didn't respond, though it did respond to a previous investigator's view which argued it should reimburse 100% of the final payment. It questioned the actions Mr B took and suggested that he had been grossly negligent in following the fraudster's instructions.
- It also pointed to the fact that the calls lasted for almost two hours (which contradicts claims of Mr B acting under pressure and in the moment) during which Mr B could have contacted ANNA using its in-app chat service. It noted that it had never spoken to Mr B on the phone before, which, along with the other red flags he identified, ought to have made him more suspicious of the call.

As no agreement was reached, the case was passed to me for a final 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.

The starting position in law is that an account holder is responsible for payments they've made themselves. Here, there's no dispute that Mr B agreed to each payment that took place. The Reimbursement Rules change that starting position for some payments that are

made as part of an APP scam. A payment service provider (like PayrNet) is expected to reimburse eligible payments unless the Exception applies. Those rules don't apply to card payments (in this case payments 1-13).

Mr B has accepted the investigator's view that, in relation to Payment 14, ANNA can rely on the Exception under the Reimbursement Rules. Because of this, and because I agree with the investigator, I will only address this point briefly after I've considered ANNA's liability for the other transactions.

While the starting position is that M Ltd will be responsible for payments 1-13, 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 ANNA should fairly and reasonably:

- have been monitoring accounts and any payments made or received to counter various risks, including 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 financial harm from fraud (among other things).
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment.

Taking that into account I've decided that:

- ANNA should have intervened by the third payment. By that point M Ltd was attempting to authorise a third payment totalling over £11,000 in a matter of minutes to a relatively high-risk merchant.
- The activity was unusual and out of keeping with the way that M Ltd's account was normally run. ANNA should have recognised that M Ltd might be at risk of financial harm from fraud.
- ANNA did provide a warning message each time Mr B approved a payment in his app. That message read:

It looks like you're trying to pay <amount> to <merchant name> on card ending <last 4 digits of the card number>.

Stop and think: Neither ANNA nor the Police will ever call you to ask you to confirm a payment like this.

Once you authorise this payment you won't have the option to recall it. If this is a scam, you may lose your money. Do you want to authorise this online payment?"

- I don't think this warning was proportionate to the risk the payments presented. It was easy to bypass and, as I understand, would appear every time a payment of this type was attempted. The risk that the third payment presented was high and ANNA needed to do more.
- I think that a proportionate intervention would have been for a member of ANNA staff to have intervened to question the payments and understand why they were being made. It could have done this, for example, using its in-app chat service.
- When attempting the faster payment, Mr B received a more detailed warning and answered a fraud questionnaire inaccurately under the direction of the fraudsters. However, I think a human intervention, earlier in the scam, was warranted and is likely to have uncovered the scam, because:

    i) A human intervention would have been able to probe the circumstances surrounding the payments. It would have been obvious to Mr B that the

intervention wasn't simply part of the payment process.

ii) Mr B says he didn't understand what the money remitter was. Had he been told he was effectively making card payments to an unknown overseas recipient, it seems unlikely he would have carried on making the payments.

iii) Mr B seems to have had doubts about the legitimacy of the caller at various points during the scam (for example by seemingly requesting a verification text message from the fraudster between payments 12 and 13). He appears to be somewhat aware of the risk that he might be falling victim to a scam. Had ANNA intervened it would have likely built on his existing doubts.

iv) Later in the scam Mr B did reach out to the genuine ANNA through its in-app chat service. This suggests he recognised the in-app chat service as being genuinely ANNA and, I think, he'd have been more likely to listen to advice received over it.

- I've also thought about Mr B's role in what happened. I've noted that there are elements of this scam that ought to have caused Mr B concern. For example, I think he might have questioned the fact he was being asked to authorise a series of card payments to secure the account. Had he done an online search for the money remitter (as he says he did in relation to the "spoofed" number), he would have seen its true nature. However, on balance, I don't think there should be a deduction from the amount ANNA reimburses that relates to the card payments, because:

  i) The fraudster appears to have attempted a payment using Mr B's card details during the call. I can see why this would have given credence to their claims that fraud was taking place. They also appeared to know some (albeit fairly limited) information about him and his business.

  ii) This type of scam preys on the victim's fear of losing their money. They have nothing to gain and seemingly a lot to lose. Their actions should be assessed in that light and, while I understand the calls went on for quite some time, it's important to recognise that Mr B wasn't given the opportunity to take a step back and consider what he was being asked to do. The fact he was contacted, unusually for ANNA, by phone may have only added to the sense that the matter required immediate attention.

  iii) The second call (before any payments took place) came from a number associated with the Financial Ombudsman Service, not ANNA. But that number does appear on ANNA's website and if an online search of the number and "ANNA" is performed (as Mr B says he did) the ANNA website is the top result. I can see how, at least superficially and during the pressure of the call, this would have suggested the caller was genuinely associated with ANNA.

  iv) The fraudsters seemed to have in-depth knowledge of how the ANNA app worked and were able to guide Mr B through the payment process. I can see why this would have given Mr B the impression he was speaking to a genuine staff member.

  v) Overall, I think his actions in relation to the card payments didn't fall far enough below what I consider to have been reasonable conduct that a deduction to M Ltd's reimbursement should be made.

- Before the point of the faster payment, it's clear Mr B had significant concerns about the legitimacy of the call. Mr B sent a series of messages to the genuine ANNA (as set out in the table above), the last of which asked for ANNA to call him because "some one has taken all my money out of my account fraudulently". He also made several calls to the Financial Ombudsman Service and although it was closed at the

time, it would have been clear who he was calling and he ought to have known that he was not being called by ANNA.

- Mr B then received a warning that touched on his exact circumstances - including being told to move money unexpectedly by someone claiming to be from ANNA. It was more detailed and specific than the warnings he received when approving the card payments.
- He also gave inaccurate answers to ANNA when it asked him about the reason for the payments. He told them the payment was for a "one-off purchase of goods and services", despite the clear reservations he had at the time about the legitimacy of the caller.
- I think that ANNA can fairly rely on the Exception to decline reimbursement for the final payment under the Reimbursement Rules. When Mr B received the warnings in relation to the final payment, he already had significant concerns about the legitimacy of the caller and I agree that, in those circumstances, it wasn't reasonable for him to have given an inaccurate reason for the payment he was making. So, I think he did move past ANNA's intervention with gross negligence.
- However, ANNA should still have prevented the payment from taking place altogether. And, unlike under the Reimbursement Rules, when considering whether Mr B also contributed to that loss, I'm required to weigh up Mr B's fault against that of ANNA. Having done so, I've found that liability should be shared for the final payment.
- I'm satisfied with ANNA's attempt to recover M Ltd's funds. It contacted the receiving firms within about an hour of the scam being reported. Given the nature of the card payments, recovery was always unlikely.

My final decision

I uphold this complaint about PayrNet Limited and instruct it to pay M Ltd:

- 100% of each disputed debit card payment after and including payment 3 – I calculate this amount to be £41,723
- 50% of the faster payment (payment 14) – I calculate this amount to be £4,500.
- Interest at 8% simple per year on those amounts from the date of the payments to the date of settlement, less any tax lawfully deductible.

Under the rules of the Financial Ombudsman Service, I'm required to ask M to accept or reject my decision before 10 April 2026.

Rich Drury
Ombudsman