DRN-4949707

The complaint

Mr R complains Penny Post Credit Union Limited (Voyager Alliance) won't refund the money he lost to a scam

What happened

In March 2022, Mr R received a call from a scammer impersonating his bank. They told him they had identified suspicious activity on his account. This tricked Mr R into thinking his account was at risk, and that he had to follow the caller's instructions to protect his funds.

During the call, it was discussed that Mr R also had an account with Voyager Alliance. The scammer, posing as his bank, said they would put him through to Voyager Alliance so it could secure his account. The follow transfers were then made/attempted from Mr R's Voyager Alliance account – resulting in a loss of almost £8,000.

- Unsuccessful transfer attempt: £7,531.44
- Unsuccessful transfer attempt: £2,500
- Successful transfer to external recipient: £2,499
- Successful transfer to the same external recipient: £5,000
- Unsuccessful transfer attempts: £420
- Internal transfer from savings: £199.50
- Successful transfer to the same external recipient: £429
- Unsuccessful transfer attempts: £5,000
- Unsuccessful transfer attempt: £3,500
- Unsuccessful transfer attempt: £1,000

A few days later, Mr R spoke to his bank and they informed him the call was a scam. He contacted Voyager Alliance to report what had happened – and subsequently complained that it wouldn't refund him. He said the payments were out of character so should have been flagged.

Voyager Alliance said the payments were authenticated via One Time Passcodes (OTPs) sent to his phone number – which he had shared, along with his passwords, with the scammers. It therefore didn't agree to refund him.

Unhappy with this response, Mr R referred the matter to our service. Our investigator looked into things and thought Voyager Alliance should refund the transactions. She didn't think Mr R had completed the payments steps himself. And in the pressure of the moment, she didn't think he understood the OTPs etc. he shared would allow the scammer to take payments from his account. In the circumstances, she thought Voyager Alliance was liable under the Payment Services Regulations 2017 (PSRs).

Voyager Alliance appealed this outcome. It said that, as a credit union, it's not under the scope of the PSRs. It also said Mr R had told it he did know payments were being taken, as he said he needed to transfer the funds to prevent fraud. And the OTP messages made it clear money would be taken. It also disagreed that the payments looked unusual.

The case was therefore passed to me to decide. I collected some further information to help me make my decision – which I've summarised below:

- I asked Voyager Alliance for records to support its assertion Mr R knew about the transfers. It said it couldn't provide anything as he said this during an unrecorded call.
- I also asked Voyager Alliance about its internal fraud processes. It said it has systems in place to flag unusual payments, as determined by the criteria it sets. These are raised with a senior manager, and – where appropriate – it will contact the member to find out more about what they are doing. None of the scam payments were flagged by these systems.
- I asked Voyager Alliance about the unsuccessful transfer attempts. It provided the following explanations:
    - £7,531.44: Breached its limit of £5,000 per transaction (it also has a limit of £10,000 per day)
    - £2,500: It's unsure why this didn't succeed, but says it could be a connection issue or due to entering the OTP incorrectly
    - £420: initially the OTP timed out (this is captured in the audit history). It says this also didn't work as there was a lag in funds being moved from Mr R's internal savings to fund the transaction meaning there were insufficient funds.
    - All later payment attempts were unsuccessful due to insufficient funds.
- I asked Mr R's bank for call recordings of him reporting the scam. I found Mr R told them the credit union caller had transferred a "significant amount" of money over to the bank, and said they would contact him a few days later for a payslip screenshot to "re-do" the funds.
- I spoke to Mr R about his memory of the scam. He said he thought it was the scammers, rather than him, who accessed his apps/online banking to make the payments. He shared his login details with them, thinking this was needed so they could complete safety checks.
  He remembered expecting a call back about his payslip, but couldn't recall the details of what this was for. I asked if he knew/thought the caller was moving money to keep his account safe. He said he did, and he was expecting them to send this back. He also explained he has some conditions which mean he gets confused dealing with finance and numbers, and had also been caught off guard at work.

I then issued my provisional decision in July 2024 explaining why I wasn't minded to uphold the complaint. In brief, that was because, as a credit union, Voyager Alliance's account didn't fall under the scope of the PSRs. I therefore didn't think the issue of whether the payments met the PSR's bar for authorisation affected its liability. I also wasn't persuaded it ought *to* have done more to protect Mr R from fraud at the time the payments were requested

I asked both parties to provide any further comments or evidence before I made my final decision. Both parties have responded, but neither has provided anything further to consider.

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 not to uphold it – for the reasons given in my provisional decision, as set out below. As I haven't received anything further to consider in response, I don't have anything further to add or address.

The investigator's outcome focussed on whether, by sharing the details he did, Mr R understood he was enabling the caller to make payments. That would be a relevant factor for considering Voyager Alliance's liability if it was covered by the PSRs. But as Regulation 3 of the PSRs explains, they don't apply to credit unions.

That means I can't rely on the provisions of the PSRs to determine liability. So the issue of whether Mr R understood the caller would be using the details he shared to make payments is not the key to whether there are fair grounds to hold Voyager Alliance liable for his loss.

Instead, I have looked at whether Voyager Alliance correctly followed its own policy and procedures when the payments were taken. I have also considered that, in line with the regulator's – the FCA's – Principles for Businesses, Voyager Alliance must conduct its business with due skill, care and diligence. By the time of these scam payments, I would expect that to include having systems in place to monitor for, and respond to, indications its members are at heightened risk of financial harm from fraud.

I have looked at the information from Voyager Alliance about the process to make these payments. It has explained Mr R's membership number, password and memorable answer were all needed to access the account. OTPs were then sent to Mr R's registered phone number to add the new payee and confirm the payments. For the payment OTPs, I understand the message would have read: *"Please use the following confirmation code XXXX to continue with the transfer of amount XX. Do not share this with anyone".*

These steps appear to have been correctly followed. The use of Mr R's personalised security detail, and codes sent to his phone, offered a layer of security. So even though I accept it was likely the scammers who used these details to access Mr R's account and request the payments, I don't think that in itself means Voyager Alliance is liable for Mr R's loss.

I would also note that, while I accept Mr R was tricked by the scammer about the circumstances, there are indications he may have known the caller would be taking payments from his account – although perhaps not the amount or number. As when he called his bank, he mentioned money being sent from his Voyager Alliance account, and seemingly thought it would be returned following completion of a check requiring his payslip. That also seems consistent with what he more recently told me about the scam.

Regardless, as explained, whether Mr R knew payments would be taken isn't key to whether Voyager Alliance holds liability for his loss. That's because I think the right process was followed to *try* to ensure the request came from Mr R (or someone with his authority). So my starting position is that Voyager Alliance is not liable as it followed the correct payment/authentication process.

However, I have also thought about whether Voyager Alliance should be held at fault for not doing more to protect Mr R from fraud at the time the payments were requested. Voyager Alliance has explained that, while it does have systems in place to look out for indications of fraud, the disputed payments weren't identified as presenting a heightened risk.

I've considered whether that seems reasonable – as if I think Voyager Alliance made a mistake, I'd consider whether that had a material impact on Mr R. In other words, if I find that Voyager Alliance ought to have taken action that was likely to have prevented Mr R's fraudulent loss, it might be fair to hold it liable.

I am conscious the payments made (and attempted) were different to how Mr R had previously used his account. The overall – and individual – payment amount(s) were higher than his usual level of account use.

However, looking at the overall character and amount of the payments in all the circumstances – thinking about the funds Mr R had in the account, and the use of his genuine security details to make the payments – I don't think the payments presented such a significant fraud risk that Voyager Alliance should be held at fault for not implementing additional checks etc. before processing the payments.

I appreciate this will be disappointing for Mr R. But I'm not persuaded Voyager Alliance is responsible for his loss due to missing a clear and obvious opportunity to prevent the scam from happening.

I'm also not persuaded Voyager Alliance ought to have been able to recover the funds. I do think it could have attempted to retrieve any remaining funds from the recipient account more quickly when the scam was reported. But bearing in mind that it was closed over the weekend when the scam occurred, and that Mr R didn't realise and report the scam until a few days later, I am not persuaded it would have been able to recover the funds. In scams like this, funds are commonly moved on very promptly to avoid recall attempts.

In saying all of this, I do want to make clear that I have no doubts Mr R has fallen victim to a scam. We know scammers will use social engineering tactics to create a sense of urgency and pressure, and will use consumers' circumstances against them, to trick them into divulging security details etc. I am also conscious of the significant amount Mr R has lost to the scam, so understand why he feels strongly about pursuing this matter. But having carefully considered all the circumstances of this complaint, I am not persuaded it would be fair to direct Voyager Alliance to refund him for his loss.

My final decision

For the reasons given above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 6 September 2024.

Rachel Loughlin
Ombudsman