DRN-5818829

The complaint

Mr R complains that Wirex Limited (Wirex) won't refund the money he lost when he fell victim to a scam.

What happened

In summary:

- Mr R had previously been a victim of a scam and lost lots of money.
- Mr R took an unexpected call from X (the scammer), who said he was a broker for Company I (the scam company) and could see the money Mr R had previously lost in a scam and he could, for a fee, release his funds.
- X and / or his accomplices then discussed a release fee through crypto payments.
- X may also have discussed crypto investments to make a profit.
- X provided Mr R with his credentials, convinced him he was legitimate and persuaded him to open an account with Wirex (a digital payment platform) so payment could be made (in crypto) to unknown accounts.
- X told Mr R there were rules to follow. This included not discussing matters with the financial firms processing the payments.
- X and / or other scammers:
    - Downloaded remote desktop software onto Mr R's laptop so they could take remote access to make crypto transfers from his Wirex account to the destination crypto exchange account(s).
    - Transfer funds from his Firm N building society account to Wirex.
    - Pay £20,000, that they'd sent to his Firm N account, to an unknown person and, when Firm N queried this, provide an untruthful cover story and a copy of a false document. Mr R was coerced into sending false correspondence (on 14 August 2023 and 8 September 2023) by the scammers and didn't want to lose his money.
- Firm N subsequently closed Mr R's account and Mr R realised he'd been scammed when he didn't hear any more from the scammers.

Mr R used his Wirex account to make the following transactions:

Transaction Number	Date	Time	Transaction Type	Description	Amount
1	11/7/23	11:07	Credit	Mr R's account	+£5,000
2	11/7/23	11:12	Exchange	Sold GBP for BTC then transferred to crypto exchange	£4,926.83 (plus £73.91 fee)
3	11/7/23	11:23	Credit	Mr R's account	+£4,792
4	11/7/23	11.23	Exchange	Sold GBP for BTC then transferred to crypto exchange	£4,721.18 (plus £70.82 fee)
5	12/7/23	10:04	Credit	Mr R's account	+£9,700
6	12/7/23	10:17	Exchange	Sold GBP for BTC then transferred to crypto exchange	£9,556.65 (plus £143.35 fee)
7	13/7/23	10:58	Credit	Mr R's account	+£10,000

8	13/7/23	10:59	Exchange	Sold GBP for BTC then transferred to crypto exchange	£9,852.21 (plus £147.79 fee)
9	13/7/23	11:08	Credit	Mr R's account	+£2,500
10	13/7/23	11:10	Exchange	Sold GBP for BTC then transferred to crypto exchange	£2,463.04 (plus £36.95 fee)
11	17/7/23	11:42	Credit	Mr R's account	+£10,000
12	17/7/23	11:49	Exchange	Sold GBP for BTC then transferred to crypto exchange	£9,852.21 (plus £147.79 fee)
13	20/7/23	09:56	Exchange	Bought GBP to BTC	+£9,725.86
14	21/7/23	15:09	Exchange	Sold GBP for BTC then transferred to crypto exchange	£9,582.12 (plus £143.74 fee)
15	28/7/23	10:29	Credit	Mr R's account	+£4,431
16	28/7/23	10:30	Exchange	Sold GBP for BTC then transferred to crypto exchange	£4,365.51 (plus £65.49 fee)
17	31/7/23	16:34	Credit	Mr R's account	+£10,000
18	31/7/23	16:35	Exchange	Sold GBP for BTC then transferred to crypto exchange	£9,852.21 (plus £147.79 fee)
19	31/7/23	16:50	Credit	Mr R's account	+£1,100
20	31/7/23	16:50	Exchange	Sold GBP for BTC then transferred to crypto exchange	£1,083.74 (plus £16.26 fee)

Mr R Complained to Wirex seeking a refund as '*they operate in a high-risk space where crypto scams are rampant' 'yet, they did nothing to stop'* the scam and recover his funds.

Wirex rejected Mr R's complaint and:

- Said he was '*sending crypto transfers to legitimate external wallets that have not been listed as scam (listed the five crypto exchanges). If you send money to scammers from the wallets in question, Wirex was not involved in that and has no information about that. We can only advise you to contact the respective companies and request information from them'.*
- Reminded him of the account terms and conditions and that it was his responsibility to never give his password to anyone, and never granting anyone access to his Wirex profile.

Mr R brought his complaint to our service. Although our investigator considered that Wirex should've intervened she didn't think an intervention would've prevented Mr R's loss.

As Mr R remains dissatisfied his complaint has been referred to me to look at.

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, although I'm very sorry to hear that Mr R has lost a significant amount of money, I'm not upholding his complaint. And I'll explain why.

My role is to independently evaluate the evidence provided by both parties. So, where evidence is incomplete, inconsistent or contradictory, as some of it is here, I must reach my decision on the balance of probabilities – in other words, what I consider most likely to have happened in light of the available evidence and wider circumstances.

In Mr R's complaint against Firm N, I wasn't persuaded that a scam has occurred. This was for the following reasons:

- Mr R hasn't been able to provide any dialogue or correspondence that he had with the scammer(s) so:
    - It is difficult to fully understand the scammers' communications (including pressure), instructions, contracts and what fully occurred. Also, how many scammers there were.
- I couldn't see the scammers' payment instructions to Mr R and where his funds went.
- The documents Mr R submitted lack clarity:
    - There was neither context or an audit trail to show when and where they came from. And for those documents, which the scammers appear to have used to persuade Mr R that his money was awaiting a return (for a fee), they are dated 14 August 2023 and 17 August 2023 which are later dates than those of Mr R's payments.
    - I couldn't see that the scammers had taken control of his laptop.
- Another inconsistency was around the scammers appearing to use Mr R as a money mule:
    - Mr R indicates the scammer sent the email to Firm N from his email account. But he also says the scammer asked him to send it.

Mr R subsequently provided video evidence of:

A. A laptop search he undertook on the broker.
B. Him talking (a one-way conversation) about the email sent to Firm N (where he appears to have been used as a money mule) and Mr R says:
    - *'Dennis' 'I just composed the letter you sent to me now and identity I hope this works. 'I don't want to lose my account'. 'I replied (or applied) the email with your own message'.*
C. Him speaking (a two-way conversation), on 4 August 2023 (after the payments in the above table), to a person who is showing and talking through screens on Mr R's laptop that this person appears to be sharing or controlling. The person shows Mr R that the payments he sent from Wirex had arrived at a crypto exchange website. Although the quality of the video is poor, which means only a few figures can be viewed, those in large font can be read and the person appears to have access to Mr R's Wirex account (as I've cross referenced a BTC rate with that on Mr R's statement). Also, the person talks about recovery of Mr R's funds.

Although some evidential gaps and remain and there appears to be a further inconsistency over Mr R remote desktop software awareness, I found the videos did add weight to Mr R's account that he was the victim of a scam. So, I considered Wirex's responsibilities and actions.

The Contingent Reimbursement Model (CRM) code doesn't apply to this case as Wirex is not a signatory and the code doen't cover cryptocurrency transactions. However, after assessing the videos, I considered Payment Services Regulations 2017 (PSR) and Consumer Duty which are relevant to this complaint.

PSR

Under the PSR and in accordance with general banking terms and conditions, Electronic Money Institution's (EMI's) should execute an authorised payment instruction without

undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There's no dispute that Mr R made the payments here, so they are considered authorised.

However, in accordance with the law, regulations and good industry practice, an EMI should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

EMI's do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions.

So, I consider Wirex should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
- Have systems in place to look for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks and EMI's are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

Consumer Duty

Also, from 31 July 2023 Wirex had to comply with the Financial Conduct Authority's (FCA's) Consumer Duty which required financial services firms to act to deliver good outcomes for their customers. Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Wirex was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. Also, look out for signs of vulnerability.

Although Mr R refers to both a previous fraud and his current vulnerability, I can't see any evidence that, prior to the 31 July 2023 payments, Wirex were aware of either.

With the above PSR and Consumer Duty in mind I considered:

Whether Wirex should've recognised Mr R was at risk of financial harm from fraud and put in place proportionate interventions?

As Mr R's account was new and in July 2023 crypto payments should've been recognised as having a heightened risk of a fraud or scam, I think Wirex should've put in place:

- An automated intervention, warning Mr R about the risk of cryptocurrency payments, upon the first payment for £4,926.83 on 11 July 2023 (transaction 2 in the table).
- A more tailored automated intervention, that covers scam risks, for the second payment of £4,721.18 also on 11 July 2023 (transaction 4 in the table).
- A human intervention, that covers scam risks and asks probing questions, for the third payment for £9,556.65 on 12 July 2023 (transaction 6 in the table).

I can't see that Wirex did any analysis, considered providing these warnings or questioned any of Mr R's payments or have provided sufficient evidence to persuade me they

intervened or that the payments weren't unusual, and it wasn't proportionate for them to intervene. If an EMI doesn't question payments that might be at risk, then it can't fulfil its duty to protect customers. I'm not saying that means it must check every payment out of its customers' accounts. But here, considering the individual circumstances of this case, I believe it ought to have provided warnings (from payment 1) and contacted Mr R (at payment 3) to check he wasn't at risk of falling victim to fraud.

I then considered:

Whether effective interventions would've prevented the losses that Mr R suffered

I've considered causation. Put simply, whether Wirex's failure to warn and intervene caused Mr R's losses. To do this, I reflected on whether any such interventions would've made any difference.

I considered what would've likely happened if:

- Crypto warnings had been given from payment 1.
- Mr R had received educational information on crypto investment scams from payment 2.
- Mr R had a communication with a Wirex fraud and scam agent at payment 3 and large transactions thereafter, who would've likely asked him a number of open questions about the:
    - Payment purpose.
    - Checks and research he had completed.
    - Expected returns and ability to withdraw.
    - Third parties or brokers advising him and their fees.
    - Third party communications.

On balance, I don't think such interventions would've either broken the spell of the scammer or uncovered a scam. I say this for the following reasons:

- The scammers had control of Mr R's device and there is evidence (from his complaint about Firm N) that they were either answering questions on his behalf or controlling his answers. So, any human intervention questions, which are electronic, would more likely than not be ineffective.
- In various call recordings on file Mr R talks about how:
    - He was aware of scams, having unfortunately fallen for a scam or scams before and had since received and dismissed many cold calls about money recovery schemes and investments as he thought they were likely to be scam calls.
    - He was convinced that he was going to get his money back and / or make a profit.
    - He felt threatened and / or harassed by the scammer(s).
    - The scammers had rules in place. These appear to be about not sharing any information about the crypto return or investment Mr R was undertaking with X and Company I. So, speaking to an agent about this would jeopardise the payments he had made, and he wanted his money back.
    - Even when Firm N confronted Mr R over a payment, where Mr R appears to have been used as a money mule, he decided not to be truthful. This includes sending or allowing a false explanation letter to go out in his name and from his email account. Also, maintaining this false account when questioned.

So, although I think Wirex should've put interventions in place to protect Mr R from financial harm I think, more likely than not, that Mr R wouldn't have told them what was really happening, and they wouldn't have unravelled the scam and prevented his loss.

Finally, I looked at whether Wirex should've done more to help Mr R recover his funds and I'm satisfied they did all they could and were sympathetic. I say this because before Mr R realised he had been scammed the funds were converted to crypto and sent to external wallets, so unfortunately there was no way for them to recover his funds. Also, as explained by our investigator, once the funds left his E-money account provided by Wirex Limited they were sent to an account which is provided by the separate company Wirex Digital Services S.r.l. who are based outside the UK and are not subject to our jurisdiction.

I realise the outcome of this complaint will come as a great disappointment to Mr R but, for the reasons I've explained, I won't be upholding this complaint and asking Wirex to make any refund.

My final decision

For the reasons mentioned above, my final decision is that I'm not upholding this complaint against Wirex Limited.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 15 October 2025.

Paul Douglas
Ombudsman