DRN-4789881

The complaint

Mr B complains that Wise Payments Limited won't refund money he lost when he was a victim of an impersonation scam.

Mr B is represented by a firm I'll refer to as 'C'.

What happened

The background to this complaint is well known to both parties and so I'll only refer to some key events here.

On 23 November 2023 Mr B received a telephone call from a person, that we now know to be a scammer, that introduced themselves as being a representative of the Supreme Court of the UK. The scammer advised Mr B that the call was in relation to HMRC as there had been allegations of fraudulent activity on his account in relation to tax. And that, to avoid going to court and paying a severe penalty, the scammer told Mr B he could pay funds into an account associated with HMRC as part of a tribunal. The scammer advised that, once paid into the bank accounts provided, HMRC would review the funds and investigate the missing tax calculation. And providing the funds were legitimate, he would receive a refund by 6:30pm.

Mr B made the following payments as part of the scam:

Date	Transaction type	Payee	Amount
23 November 2023	Fund transfer	'D'	£1,000
23 November 2023	Fund transfer	'M'	£1,537
23 November 2023	Fund transfer	'M'	£460
23 November 2023	Fund transfer	'M'	£1,000
23 November 2023	Fund transfer	'D'	£1,000
23 November 2023	Fund transfer	'R'	£2,000
		Total	£6,997

Mr B realised he was scammed when he didn't receive a subsequent call, as he was told he would, from the scammer. So, he called the official Supreme Court number and after explaining what happened he was informed he'd fallen victim to a scam.

C complained, on Mr B's behalf, to Wise on 8 January 2024 saying the payments were made as part of a scam. In short, they said:

- The scammer called Mr B from a telephone number associated with the Supreme court to provide their legitimacy. Mr B checked this on Google and found the telephone number was used by the Supreme Court. Unaware of sophisticated spoofing techniques used by scammers, Mr B thought this was genuine.
- Mr B noted the professional tone of the scammer and had no reason to question their authenticity. And as Mr B had recently made a refund to HRMC regarding an overpayment for the universal credit he received during the pandemic, he believed it

could've been linked to the financial crime investigation the scammer informed him of.

- Mr B was in a pressured situation heightened by the prospect of losing his entire life savings. And he was convinced by the scammer due to them successfully spoofing a genuine contact number and putting forward a reasonable story – which, in the heat of the moment, convinced Mr B nothing was amiss.
- Given the frequency of the payments being sent to new and unusual payees, it is expected that Wise would have effectively intervened and contacted Mr B to discuss them further. But the only intervention Mr B received from Wise was a pop-up message that was easily bypassed.
- These payments were highly unusual for Mr B's account when compared to his usual financial activity – with the account opened in September 2023.
- If Wise had contacted Mr B to have discussed the payments, then basic questioning surrounding the transactions would've established the funds were being moved for HMRC security reasons. This would've immediately been recognised as an impersonation scam and prevented it from escalating further.
- Mr B says he wouldn't have proceeded to make further payments if Wise had effectively educated him on the high risks of scams like this.
- To settle this complaint, Mr B would accept a full reimbursement of his losses, 8% interest and £300 compensation.

Wise didn't uphold the complaint. In short, they said:

- They provided Mr B with scam warnings, making him aware it could be a scam, and prompted him to specify the reason for the transfers. The reason for these warnings is to try to raise customer awareness about scams – as they've seen a rise recently – and they want to check if the transfers are associated with a scam, along with giving customers extra time to be sure they're happy to proceed.
- Mr B selected 'friends and family' as the purpose of these transfers and so, they showed him further advice which included:

  "Have you met [name] in real life?
  Scammers often create fake profiles online to trick people into giving them money. If you haven't met them in person, it's safest not to give them money.

  Did [name] ask for money unexpectedly?
  If you got a message on social media, it could be a scammer who's hacked [name's] *account. Double check with them before paying."*

  After reading this advice, Mr B proceeded to confirm the payments.
- They verified the receiving accounts of D and R as per the requirements that are set to financial institutions. And they investigate all scam reports upon receipt but they didn't know these payments were made as part of a scam until after the situation was reported to them – when the money had already been received by the scammers.
- M is a customer of a recipient bank, not Wise. And once a transfer is sent to a recipient bank, the funds are no longer under their control.

- The obligations of ensuring the legitimacy of the recipient lies with the sender of the payment. Consequently, they always recommend that their customers perform their own investigations on that person or business before setting up a payment. This fact is expressed multiple times in various parts of their system – including their help centre and section 29.1 of their customer agreement.
- They cannot be held liable for any circumstances beyond their control – such as when a loss occurs because of fraudulent behaviour on behalf of the recipient after a payment has been made to them
- After this fraud was reported to them on 23 November 2023, they took action on their end by blocking the recipients to prevent further fraudulent payments through their platform. And despite trying to recover Mr B's funds, which they can't guarantee, they haven't been able to so far.
- They completed the transfers as directed and, therefore, fulfilled their contractual obligations.

Mr B's complaint was referred to the Financial Ombudsman. Our Investigator didn't however think Wise had to do anything further. She said as Mr B's account had only recently been opened and had minimal usage before the scam, Wise were unable to determine his usual spending activity. And while the payments may have been of a high value collectively, given Mr B confirmed they were going to friends and family, they wouldn't have appeared as unusual to Wise for them to have been concerned he was at risk of financial harm.

Our Investigator also explained that, while Mr B may have been told by the scammer to select friends and family as the payment purpose, this prevented Wise from knowing the genuine payment reason and being able to provide a more appropriate warning. So, she wouldn't have expected Wise to have done anything more as they wouldn't have had reason to think Mr B was at risk of falling victim to a scam. Our Investigator further added that Wise contacted the beneficiary's banks to see if any funds remained, as she would expect them to, but unfortunately no funds remained.

C disagreed and asked for Mr B's complaint to be reviewed by an Ombudsman. The matter has therefore been passed to me to decide. C, in short, added:

- They queried what transactions Mr B put friends and family for, and what other options were available for Mr B to select.
- It is unfair to deny Wise liability as there was unusual activity and so, they had a duty to act. And although Wise isn't a signatory of the Contingent Reimbursement Model (CRM) code, there is a level of standard practice that they must uphold.
- Mr B made six payments in quick succession to four new payees. And so, Wise ought to have been on notice, regardless of the payment purpose that was selected, and should have asked Mr B probing questions about the transactions. Had they done so, there would have been further opportunities for Wise to detect the scam.

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.

I'm sorry Mr B has been the victim of a scam and I don't underestimate the impact this has had on him. But while I'm sympathetic to Mr B's circumstances, I must consider whether

Wise is responsible for the loss he has suffered. I know this won't be the outcome Mr B is hoping for but, for similar reasons as our Investigator, I don't think they are. And so, I don't think Wise has acted unfairly by not refunding the payments. I'll explain why.

I've thought about the CRM code which can offer a potential means of obtaining a refund following scams like this one. But as Wise isn't a signatory of the CRM code, these payments aren't covered under it. I've therefore considered whether Wise should reimburse Mr B under any of their other obligations.

In broad terms, the starting position in law is that an electronic money institution (EMI) is expected to process payments that their customer authorises them to make. It isn't disputed that Mr B knowingly made the payments from his account – albeit under the direction of the scammer – and so, I'm satisfied he authorised them. Therefore, under the Payment Services Regulations 2017 and the terms of his account, Wise are expected to process Mr B's payments and he is presumed liable for the loss in the first instance.

However, taking into account the regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for Wise to take additional steps or make additional checks before processing a payment to help protect customers from the possibility of financial harm from fraud.

Here, as part of the transfer process for the payments, Wise warned Mr B that it could be a scam and asked him to tell them what the transfers were for so they could provide advice. On the instruction of the scammer, Mr B selected 'friends and family' as the purpose of the payments – which, naturally, generated scam warnings associated with that type of risk and so it wasn't particularly relevant to Mr B's circumstances. This, however, was of no fault of Wise's as they wouldn't have been able to identify from the payees that the payments were for other purposes.

There were however other options Mr B could've selected that would've more accurately described the purpose of the payments – these are 'paying a bill (eg. Utilities or tax)' and 'something else', with the latter option allowing Mr B to enter a customer payment reason. Had Mr B selected either of these options it would've given Wise a better understanding of the payments – thereby allowing them to provide him a more tailored scam warning, such as one associated with the risks of paying tax. It also could've helped them identify whether they ought to have taken additional steps to try and protect Mr B from a scam. Unfortunately, due to Mr B selecting an inaccurate payment reason, they were prevented from knowing the true purpose of the payments. And so, I don't think Wise acted unreasonably by providing the scam warning they did.

I've thought about whether Wise ought to have taken further steps beyond providing these warnings. When considering this, I've kept in mind that EMIs process high volumes of transactions each day. And that there is a balance for Wise to find between allowing customers to be able to use their account and questioning transactions to confirm they're legitimate. And as Mr B had only opened the account about two months prior, with minimal account activity prior to the scam payments, Wise would've been unable to establish whether the payments were out of character based on his typical account usage.

Although collectively, the payments were for a relatively high amount, they were individually quite low value and sent to several different payees. And with Mr B providing the reason for the payments as being for friends and family, I don't think this would've necessarily stood out to Wise as being unusual account activity. But rather, it would've appeared as genuine account activity – as it's not uncommon for customers to legitimately send money to friends

and family. And while the scam payments were made on the same day, within a relatively short period of time, I don't think they were so unusual or suspicious whereby I would've expected Wise to have been concerned that Mr B was at significant risk of financial harm from fraud. Because of this, I wouldn't have expected Wise to have carried out additional checks before processing them. I'm satisfied the online scam warnings Wise presented – based on the payment purpose Mr B provided – was appropriate and proportionate to the risk identifiable to them at the time.

I've considered whether, on being alerted to the scam, Wise could reasonably have done anything more to recover Mr B's losses, but I don't think they could. This is because Wise, and the beneficiary account provider, have shown that the funds were removed from the payee's accounts before the scam was reported. And so, although Wise did attempt to the recover funds as I'd expect in the circumstances, there was no funds remaining for them to recover at the point they became aware Mr B had been scammed.

I have a great deal of sympathy for Mr B and the loss he's suffered, as I appreciate it is a significant sum of money to him. But it would only be fair for me to direct Wise to refund his loss if I thought they were responsible – and I'm not persuaded that this was the case. For the above reasons, I think Wise has acted fairly and so I'm not going to tell them to do anything further.

My final decision

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 B to accept or reject my decision before 18 July 2024.

Daniel O'Dell
Ombudsman