DRN-3403834

The complaint

Mr M complains that Wise Payments Limited (previously TransferWise Limited) ("Wise") won't refund money he lost to a scam.

Mr M is being represented by his son in this complaint.

What happened

In 2019, Mr M was the victim of an investment scam. He read an article about cryptocurrency and forex trading by a recognised Danish CEO on social media, which endorsed a broker called TraderUR. Mr M's son says that Mr M was likely targeted as he was researching for ways to grow his money.

After leaving his contact details on a web form, Mr M was contacted by a representative of TraderUR who claimed to be able to help him invest money and make a reasonable profit. Mr M was told that any funds transferred would still belong to him and in the worst case he could only lose 5% on a deal. He also received an action plan which he thought was reasonably sensible.

Mr M was persuaded to engage the services of TraderUR and opened a trading account with it. The representative also asked him to set up a multi-currency electronic money account with Wise to fund the deposits. Mr M would send Danish Krone from his bank account in Denmark to his Wise account, and it was converted to Euro before being sent to TraderUR's account in another EU country.

Mr M says that once transactions started, he would get regular calls from his account representative who would ask for more money. Things looked promising and his profits exceeded the action plan he was initially given. After a few transactions, Mr M was contacted by another representative who persuaded him to download a screen-sharing software to help arrange transfers while on the phone to him. Mr M's submissions also suggests that he was able to make a few withdrawals from his trading account.

The following payments were made from Mr M's Wise account to TraderUR:

Date	Payee	Amount
18 March 2019	Shine Systems Kft.	400,000 DKK (€53,393.81)
20 March 2019	Shine Systems Kft.	400,000 DKK (€53,405.77)
22 March 2019	Rumolis Grand Kft	500,000 DKK (€66,757.37)
25 March 2019	Shine Systems Kft	500,000 DKK (€66,737.44)
26 March 2019	Rumolis Grand Kft	500,000 DKK (€66,737.44)
28 March 2019	Rumolis Grand Kft	500,000 DKK (€66,717.51)
4 April 2019	Rumolis Grand Kft	450,000 DKK (€60,063.63)
8 April 2019	Rumolis Grand Kft	450,000 DKK (€60,054.67)
	Total payments	3,700,000 DKK (€493,867.64)

Wise wrote to Mr M on 9 April 2019 and requested further information about these payments. It also said it was unable to process any future transactions unless it received a satisfactory response. Mr M replied the same day, but his response didn't address everything.

Wise sent a few email chasers and also contacted Mr M to discuss its request. It had further questions after Mr M provided additional documentation. Wise deactivated Mr M's account on 3 May, after it didn't receive a satisfactory response.

During this period, Mr M had been in touch with his account representative at TraderUR. The representative persuaded him to open an account with another online money remittance firm and Mr M continued sending money to his trading account. The available information suggests that Mr M made the first payment to TraderUR through a different firm on 12 April – three days after Wise got in touch with him to question the payments.

According to Mr M's submissions, things went quiet when he started losing money on his trading positions. He eventually heard back from the initial representative who asked him to deposit €60,000 to recover the losses. This request for additional deposit appears to have happened around early May, based on the email exchange between Mr M and TraderUR which was included in his submissions.

But by this point, Mr M had realised this was a scam. He requested a withdrawal of his deposits, less what had he had already received. He also reported the matter to the police and his bank.

Mr M contacted Wise on 15 May and explained that he'd been the victim of a scam. He asked for its assistance in recovering the funds. Wise agreed to co-operate with any institutions investigating the matter, including the police, if contacted. But it refused to provide a refund as it didn't agree it had done anything wrong. Mr M complained to Wise and when he didn't hear back, the matter was referred to our service.

I issued my provisional decision on 10 March 2022. I said that I didn't plan to uphold this complaint and set out the following reasons:

> *Mr M and his family have gone through a difficult time in the last few years and I acknowledge that this complaint is very important to them. I thank them for their patience and for taking the time to give us all the details they have.*
>
> *I've first thought about our service's territorial remit and what it means for Mr M's complaint. Both the sender (Mr M) and the recipient (beneficiary) are based outside the UK, and the payments were conducted outside the UK. I sought clarification from Wise in relation to the payment journey involved in such transactions which it kindly provided. Wise also said it was satisfied from its own point of view that our service can consider Mr M's complaint.*
>
> *I've reviewed the information Wise has provided in relation to the payment journey. At the time of the disputed payments, Wise passported out its services to EEA countries under permissions granted to it by the Financial Conduct Authority ("FCA"), the UK's financial services regulator. Although the payments were seemingly conducted outside the UK, the payment instruction – the request to make a payment transfer – was received and actioned in the UK by Wise. I'm therefore satisfied that Mr M's complaint falls within our service's territorial jurisdiction.*
>
> *Given the information I've found during my research on TraderUR, I'm satisfied that Mr M has likely been the victim of a scam, rather than simply losing money as a*

result of a high-risk investment. There are warnings published about TraderUR by the International Organisations of Securities Commissions ("IOSCO") as well as by the FCA, albeit several months after Mr M made all the payments he disputes.

It's common ground that Mr M authorised the payments even though he was the victim of a sophisticated scam. He was duped into instructing Wise to transfer money to the accounts within the fraudster's control. Although he didn't intend the money to go to the fraudsters, under the relevant regulations, Mr M is presumed liable for the loss in the first instance. But that's not the end of the matter.

Regulatory framework

Wise is an electronic money institution ("EMI") and its FCA permissions are different to those of a bank or a building society. EMIs and authorised payment institutions ("PI") operate differently and in a different regulatory framework. In broad terms, the well-established codes of practice for fraud prevention don't apply in the same way to EMIs and PIs as they do to banks and building societies.

Strictly speaking, publications and codes aimed at banks and building societies either don't apply or have limited application to EMIs and PIs. Particularly if the transactions in question happened several years ago. An example of a code that doesn't apply to EMIs and PIs is the Banking Protocol. It is only relevant to in-branch transactions, whereas EMIs and PIs tend to offer services online or over the phone. It's also important to note that some considerations which have long applied to banks and building societies have only come into force more recently for EMIs and PIs. For instance, the FCA's Principles for Business (PRIN) and Conduct of Business sourcebook (BCOBS) have only applied to EMIs and PIs since August 2019.

But even before this date, as is the case here since Mr M made the payments in March and April 2019, EMIs and PIs still owed a basic duty of care to their customers, as well as a duty to mitigate fraud.

I've thought carefully about Wise's obligations in Mr M's case.

Should the payments have flagged as unusual or out of character?

I accept that Mr M's use of Wise's services was broadly in line with what it would expect – a customer opening and funding an account specifically to make international payments. So, on the face of it, the fact that Mr M deposited money into his account just a day or two after opening it and then sent that money on internationally is unlikely to have stood out as being remarkable, suspicious or unusual activity to Wise.

However, the payment in question was of a substantial amount – equivalent to over £50,000. I acknowledge that Wise may well have processed over 70,000 transactions over £50,000 in 2019. But Mr M was a new customer and Wise didn't have any account history to compare the transaction against. In the circumstances, it is my judgement that the initial transaction alone ought to have triggered an alert on Wise's systems.

Wise has argued that money deposited from a legitimate bank account implies that the bank has done its due diligence and knows its customer, and Wise considers such payments more trustworthy. I can understand its logic to some extent. But where the customer is new to Wise, in my opinion relying on the deposit being received from a legitimate bank account in the customer's name doesn't go far

enough. After all, as has happened with Mr M, a fraudster can convince an individual to open a new account with an EMI (like Wise) to facilitate fraud. And when the initial payment that follows is of a substantially large amount, like it was here, I consider it ought to stand out as unusual and prompt further enquiries.

So, I think an opportunity was missed here.

Would intervention have prevented the fraud?

The investigator thought that Wise should have asked questions along the lines suggested in the British Standards Institute (BSI) code which came into effect at the end of October 2017. It is worth noting that EMIs and PIs weren't involved in this code's creation. As time has gone on, I consider the code represents good industry practice not just for banks but also other types of payment service providers. But I don't think the same can be said in relation to EMIs and PIs for payments made in March-April 2019, which is just 17-18 months after the BSI code came into effect.

In other words, I wouldn't have expected Wise to have questioned Mr M to the extent suggested in the BSI code. If Mr M had disclosed the circumstances of his introduction to the investment of his own volition, I would have expected Wise to have been on notice that he was at risk of financial harm from fraud. But having weighed up everything, I'm not persuaded that Mr M would have been forthcoming with this information.

The scam had a high degree of sophistication and it's one that Mr M was clearly very taken in by. His son has told us that the fraudster approached Mr M with care, reassurances, and lots of guarantees. And Mr M's submission is that he was convinced by the fraudster's eloquence and thought that the action plan was sensible.

When Wise subsequently questioned Mr M about the payments, he got in touch with the fraudster and informed them of this. And the fraudster convinced Mr M to not only open an account with another firm (and no longer use Wise) but also continue sending money to them. Although Mr M did respond to some of Wise's questions, including the reason for the payments, he didn't say that it was for investment trading. So, if Wise had intervened when Mr M authorised the initial payment, I think it's more likely than not that similar actions would have unfolded. Mr M would have reported this to the fraudster, and the fraudster would have convinced him to make payments through another firm.

I'm also mindful that Mr M's son has told us that he had a difficult time convincing Mr M this was a scam. So, even if Wise had provided a warning about scams in general (which is all I could expect of it in the circumstances), I don't think this would have made a difference to whether Mr M would have gone ahead with the payments.

So, while I've found that Wise could have done more here, I'm persuaded that any intervention by Wise would likely have been ineffective.

Was enough done to recover Mr M's funds?

Wise has told us that it didn't attempt to recover the funds Mr M had stolen from him.

Wise is expected to assist its customers in recovering misappropriated or misdirected funds when put on notice. So, I consider that it ought to have attempted recovery when Mr M got in touch to report the fraud.

That said, there's no guarantee that the international beneficiary bank would have responded to a recovery request. Indeed, our investigator reached out to the beneficiary bank in this case to find out if the funds remained in the account at the point when Mr M reported the fraud. But he never received a response.

Also, fraudsters are very much alive to the processes financial businesses take when being made aware of fraud. To prevent the funds from being frozen and returned to the victim, fraudsters tend to remove the funds from the beneficiary account within a short period of being credited. As Mr M didn't report the fraud to Wise until several weeks after his last payment through Wise, I find it more likely than not that the funds were removed prior to this.

As such, I don't find that recovery in these circumstances would likely have been successful even if Wise had acted like I think it should have.

Complaint handling

In its submissions, Wise said it wanted to offer compensation to Mr M as it had failed to send a final response when he complained. During our investigator's review, an offer of £150 was put forward. But given that complaint handling isn't a regulated activity, I'm unable to comment on any offer of compensation in relation to it. I leave it to Mr M to contact Wise directly if he wants to accept its offer.

I invited further comments and evidence from both parties.

We haven't heard from Wise, so I've assumed it has nothing further to add.

Mr M's son has replied. In summary, he says that I've rejected the complaint based on assumptions and this is unfair. He agrees Wise doesn't have the same responsibilities to monitor accounts as a bank does. But where opportunities are missed, Wise must be held liable to some extent. He says that all regulations are applicable and presumes that 17-18 months is more than enough time for the BSI code to be implemented by every financial institution in the UK. He's also quoted a response from the Electronic Money Association ("EMA"), which Wise is a member of, to the APP Scams Steering Group's 2018 Consultation Paper on the Contingent Reimbursement Model ("CRM") code; specifically its response to customer vulnerability. He says the response makes it clear that Wise leaves it to the Financial Ombudsman Service to decide vulnerability and therefore retrospectively reimburse customers.

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 thank Mr M's son for his comments which I've read and considered in their entirety. I recognise that he feels strongly about the matter and that he's disappointed with my decision.

I've reviewed Mr M's case again taking into account further comments that his son has put forward. My outcome, as set out in my provisional decision, remains unchanged. I've answered the key further points below.

Causation is a critical determinative factor in every fraud case. It isn't enough that a payment service provider failed to act unfairly or unreasonably; its acts or omissions must be the

immediate and effective cause of losses that were reasonably foreseeable at the time of the breach. So while I've made a finding that Wise missed an opportunity to intervene and provide a warning to Mr M, this doesn't mean it automatically becomes responsible for his loss. I would also need to be satisfied that the 'breach' would have made a difference to Mr M's decision-making.

I can't know for certain what would have happened if Wise had questioned Mr M about the initial payment before executing it. In such situations, I reach my conclusions not based on mere possibilities but rather on what I find most probable to have happened in the circumstances. In other words, I make my decision based on the balance of probabilities – so what I consider most likely to have happened considering the evidence and wider circumstances of the case. This includes taking into consideration actions that *were* taken.

As I set out in my provisional decision, Mr M contacted the fraudster when Wise subsequently questioned the payments that he sent using its services. Within days he was using the services of another e-money provider to continue sending money to his trading account. I've also noted that Mr M's son has said he had a difficult time convincing his father that this was a scam.

Based on these actions, it remains the case I consider it more likely than not that any contact or further discussion with Wise at the time Mr M authorised the payments would not have stopped him from going ahead. Therefore, any failure on Wise's part in relation to not spotting the disputed payments as unusual or out of character is not the dominant, effective cause of Mr M's loss.

I understand the point Mr M's son is making about the EMA's response to the APP Scams Steering Group. But it's worth noting that this response was in the context of a Consultation Paper on the CRM code. This code: didn't come into force until 28 May 2019 (or the date the respondent firm signed up to it if later); is voluntary; isn't retrospective; only applies to authorised push payments between two accounts held in the UK and not by the same person. The CRM code, therefore, doesn't apply to Mr M's case.

In any event, as I've found that an intervention is unlikely to have made a difference here, I don't consider it necessary to comment further on the regulatory framework and the obligations of EMIs and PIs in fraud prevention.

In summary, I know that Mr M and his son will be disappointed with this outcome. Not least because the matter has been ongoing for some time and our investigator previously upheld the complaint. I acknowledge that Mr M has experienced personal difficulties since losing a very large amount of money to a cruel scam. But having considered the matter carefully, I don't think that Wise could have prevented the losses he suffered.

My final decision

For the reasons given, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M (or his representative) to accept or reject my decision before 27 April 2022.

Gagandeep Singh
Ombudsman