

The complaint

Mr K complains that TTT Moneycorp Ltd hasn't refunded him after he fell victim to a holiday accommodation scam.

What happened

Mr K fell victim to a scam in April 2022 when trying to book accommodation abroad.

I issued a provisional decision for this complaint on 16 February 2024. I've copied the text at the end of this final decision (*in italics*) and so I won't repeat all the background, findings, and reasoning again here. Instead, I'll focus on the developments since the provisional decision.

Mr K didn't respond to the provisional decision, so there's nothing more for me to consider from him.

Moneycorp did respond and didn't accept the findings. In summary, it said:

- It was under no obligation to question the payment made by Mr K. It further referred to the *Phillip vs Barclays Bank UK PLC* judgment in its response;
- It didn't believe the payment made by Mr K was unusual account activity for him;
- There had been enough warnings given, which were of sufficient quality, so as to deter Mr K from proceeding;
- Moneycorp knew very little about the payment and couldn't have known it was being made toward a scam; *and*
- Mr K didn't act reasonably in the circumstances.

I'm now issuing my final decision to address the arguments made in response to the provisional 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.

I'm upholding the complaint and for the same reasons as explained in my provisional decision. I've carefully considered all Moneycorp has said, but I'm not persuaded to change the outcome.

Whilst Moneycorp's response to the provisional decision was quite extensive, with various parts of the *Phillip vs Barclays Bank UK PLC* judgement referred to, I won't be addressing every point raised. I have considered everything, but I've already explained my reasoning around the *Phillip* judgement, and Moneycorp's more recent response reveals nothing new.

I remain satisfied that Moneycorp's terms and conditions gave it the right to stop suspicious payments for questioning. Such interventions are commonplace across the industry and widely carried out by firms regulated under the Payment Service Regulations (2017). They are accepted as good practice and the FCA has talked frequently about the importance of scam prevention and customer protection. I have taken account of the relevant regulations and law (including case law) in reaching my decision. But I have also taken account of industry best practice and what I can consider to be fair and reasonable in all the circumstances of the case.

I also remain satisfied the payment made toward the scam was sufficiently unusual that it would have been fair and reasonable for Moneycorp to question. That position is strengthened by the fact Moneycorp were engaging with Mr K directly about the payment. This wasn't a case of Mr K submitting the payment instruction with no interaction with staff.

Whilst it is true Mr K carried out several high value currency purchases on his account, I've seen little evidence of high value external payments to new payees.

The warnings Moneycorp gave during the payment process were very light touch and, as I've said before, didn't bring to life common features of scams. Moneycorp has said it isn't necessary – perhaps even undesirable – for warnings to contain such detail. I disagree. Whilst there is a balance to be struck, and a warning shouldn't be so long and detailed that it loses a customer's attention, there must be features that resonate with a customer's circumstances if such warnings are to have any effect. What's more, I'm satisfied here that a tailored intervention was necessary, with Mr K being questioned about the purposes of the payment, given the scam risks attributable to it. Clearly that didn't happen here when it fairly and reasonably ought to have done.

Importantly, Moneycorp was discussing the payment with Mr K. So it did know – or ought to have known – more than the very basic details of the transaction. I don't accept Moneycorp's argument that there was no way it could have picked up on some of the hallmarks of a scam like this. It was the professional in this relationship and ought to be well-versed in identifying when a customer is at risk of financial harm through fraud. There were enough early signs presented to Moneycorp that it ought fairly and reasonably to have questioned Mr K further about the purpose of his payment, how he found the accommodation, and what had transpired since finding it. That is how the fuller details would have been revealed to Moneycorp and where a more detailed and tailored warning could have been given to Mr K, with the impartation of Moneycorp's expert knowledge about the risks of scams like this.

Moneycorp has also said Mr K's actions weren't reasonable. I'd said as much in my provisional decision, and it is why liability is shared. The actions of both parties must fairly and reasonably be taken into account.

Putting things right

The award I intend to make is as follows:

- A refund of 50% of the funds lost to the scam;
- Payment of interest on that refund at 8% simple per year, calculated from the date of loss to the date of settlement

My final decision

I uphold this complaint against TTT Moneycorp Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 9 April 2024.

The provisional decision is copied below

I've considered the relevant information about this complaint.

Having done so I'm upholding the complaint, but the overall outcome differs to that recommended by our investigator.

I'll look at any more comments and evidence that I get by 1 March 2024. But unless the information changes my mind, my final decision is likely to be along the following lines.

The complaint

Mr K complains that TTT Moneycorp Ltd hasn't refunded him after he fell victim to a holiday accommodation scam.

What happened

The background to this complaint is well-known to both parties and so I won't go into extensive detail here.

In April 2022 Mr K was looking for a holiday property to rent in the South of France. He found a place that he liked on a villa rental website. The advert asked interested parties to get in touch with the host directly and gave an email address. So that's what Mr K did.

What Mr K didn't know at the time was that he was entering into correspondence with a scammer.

Mr K emailed back and forth with the scammer, going through enquiries about: availability, length of stay, cost and so on. This resulted in Mr K looking to secure a booking for a month at a cost of EUR12,280. The scammer told Mr K he'd be contacted by the sister company of the villa rental site to confirm the booking and make payment. They said this was because it was the French version of the UK website.

Mr K did receive the payment instructions as promised. But the emails were fake, copying and cloning details of a genuine firm to make them look legitimate.

Mr K attempted to complete the payment with Moneycorp online, but the account details wouldn't work. The scammer sent him a new set. Mr K also had trouble with these and so called Moneycorp to make the payment. A couple of days later the payment still hadn't gone through and so Mr K called again.

Moneycorp told Mr K it needed email confirmation of the account details and so he sent those through. The payment was then completed on the phone, with the money actually being sent the following day.

Mr K had some follow-up questions about the booking and so contacted the scammer again, but they were unresponsive. After several failed attempts at contact Mr K got in touch with the original villa booking site. It said they had no details about Mr K's booking and the scam was revealed.

Mr K reported what had happened to Moneycorp. It tried to recover Mr K's money but was unsuccessful. It said it couldn't help any further and said it wouldn't refund Mr K.

Unhappy with Moneycorp's response Mr K contacted our service. One of our investigators considered what had happened and recommended the complaint be upheld. He did so on the basis that:

- *Moneycorp ought fairly and reasonably to have been on the lookout for unusual and*

suspicious account activity that might be linked to fraud and which might put Mr K at risk of financial harm;

- *Mr K's payment was of a high value and out of character compared to his normal spending, meaning Moneycorp ought to have questioned him about it;*
- *In making that finding the investigator noted Moneycorp spoke with Mr K on the phone and so had a good opportunity to discuss the payment and warn against the type of scam Mr K was falling victim to;*
- *The investigator could also see Moneycorp had been sent a copy of the payment instruction sent by the scammer, which it could have looked at and likely recognised the hallmarks of a scam.*
- *Mr K's own actions were reasonable, given the communication with the scammer wasn't alarming and that what appeared to be genuine payment instructions had been received.*
- *The investigator recognised some warnings were presented to Mr K when he tried to make payment online. But he didn't believe these went far enough or made clear the common features of scams like this.*

Our investigator said Moneycorp ought to refund Mr K's loss in full and pay interest at 8% simple per year.

Moneycorp disagreed. In summary, it said:

- *There was no duty on it to intervene and stop Mr K's payment instruction for questioning when it appeared otherwise legitimately authorised. It referenced the case of Philipp vs Barclays Bank UK PLC [2023] UKSC 25 in its response, saying it had a contractual duty to make Mr K's payment.*
- *It did not believe the payment made by Mr K was out of the ordinary when compared to normal account activity.*
- *Mr K had contacted the scammer outside of the villa rental website's normal channels which was expressly against its warnings. Payment had also been made outside of its checkout/booking process.*
- *Mr K had ignored the online warnings it had given about scams.*

As an outcome hasn't been agreed the complaint has been passed to me for a review and, ultimately, a final decision.

What I've provisionally 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.

Unless there's significant new evidence or information that's presented by either party, my final decision will follow along these lines.

I intend to uphold this complaint, but with a different overall outcome to that recommended by our investigator. I find each party should share responsibility for the loss on a 50:50 basis. I'll explain why. In reaching these findings I won't necessarily comment on all points made by Moneycorp and Mr, though I have considered everything we've been given.

Should Moneycorp have questioned the payment Mr K was making?

There's no dispute that Mr K authorised the payment himself. And so, under the Payment Service Regulations (2017) he is deemed responsible for it, even though he gave authorisation under false pretences. This is the starting legal position and the case of Philipp

vs Barclays Bank UK confirmed that account providers, like Moneycorp, have a contractual duty to follow a customer's payment instruction.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by firms when making payments. Among other things, it said, in summary:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a firm to make a payment, the firm must carry out the instruction promptly. It is not for the firm to concern itself with the wisdom or risk of its customer's payment decisions.*
- The express terms of the current account contract may modify or alter that position. For example, in Philipp, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a duty to do so.*

In this case, Moneycorp's terms and conditions conferred on it rights (but not obligations) to:

- Attempt to contact the customer using a secure method in order to discuss any suspicious or fraudulent activity it suspects on the customer's account.*

So the starting position at law was that:

- Moneycorp was under an implied duty at law to make payments promptly.*
- It had a contractual right not to make payments where it suspected fraud.*
- It had a contractual right to delay payments to make enquiries where it suspected fraud.*
- It could therefore refuse payments, or make enquiries, where it suspected fraud, but it was not under a contractual duty to do either of those things.*

Whilst the terms and conditions did not oblige Moneycorp to make fraud checks, I do not consider any of these things (including the implied basic legal duty to make payments promptly) precluded Moneycorp from making fraud checks before making a payment.

And whilst Moneycorp was not required or obliged under the contract to make checks, I am satisfied that, taking into account longstanding regulatory expectations and requirements, and what I consider to have been good practice at the time, it should fairly and reasonably have been on the look-out for the possibility of APP fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances – as in practice all account providers, including Moneycorp, do.

In its submissions to this service, Moneycorp has also confirmed:

Moneycorp has policies, procedures and controls to mitigate financial crime risk, protect its customers and the firm whilst complying with our regulatory obligations. Moneycorp's financial crime policies, procedures and program is subject to regular independent review and audit and staff members are regularly trained on how to recognise suspicious or unusual activity. Additional rules and safeguards are embedded within our systems to detect and enhance fraud prevention and to educate customers on fraud risks.

Moneycorp undertake due diligence on new and existing accounts, monitor transactions, and conduct regular screening of beneficiaries for the purpose of detecting financial crime (including, but not limited, to fraud).

With all of this in mind, in this case I'm satisfied Moneycorp ought fairly and reasonably have questioned the payment being Made by Mr K on the basis that:

- It was a significant sum of money being sent;*
- It appears to have been one of the largest outgoing payments from his account since*

it was opened;

- *The payee was new and untested;*
- *Mr K rarely – if ever – sent money to anyone other than himself. It doesn't appear there were any other payees created on his account;*
- *Mr K had been trying and failing to set up the new payee, completely changing account details part-way through.*

In making these findings it's important to consider the above points aren't to be taken as stand-alone considerations. They ought to merge to form the overall risk picture. But there's more to consider, beyond this detail.

The fact is that Moneycorp was speaking to Mr K on the phone about his payment. It ought fairly and reasonably already have been considering the payment as out of character and so questioning it. But given Mr K was engaged in a direct interaction with a member of staff (possibly on two occasions) there was clearly an opportunity for Moneycorp to act and protect Mr K from financial harm.

It is also true that further details about the payment were revealed to Moneycorp. These details represented typical hallmarks of a holiday property scam. As the professional in the relationship, Moneycorp ought fairly and reasonably have recognised these hallmarks and questioned Mr K further.

- *Moneycorp knew Mr K had received the account details by email, but didn't question him further on this;*
- *Moneycorp could see the booking was allegedly with a holiday rental provider, but that payment was being made by transfer (rather than card payment);*
- *Moneycorp knew a business was meant to be paid but could see the account was that of an individual.*

These are indicators that did not require investigation. They naturally presented themselves as the payment was being processed by Moneycorp. And so they ought to have contributed to Moneycorp's sense of concern and led to an intervention and questioning of Mr K.

It's not for me to say exactly what Moneycorp should have asked. But it's fair and reasonable to suggest it could have gone through the detail about how Mr K had found the villa, how he'd been communicating about the booking, and why he was paying an individual. There appears to be no reason Mr K would have lied. And so it's fair and reasonable to say Moneycorp would have been able to recognise a scam was taking place and warn Mr K against proceeding, highlighting the specific features of such scams. There's no evidence to suggest Mr K wouldn't have then heeded that warning.

Moneycorp has referred to the warnings it did give. But I, like our investigator, don't find these to have been sufficient. None went into the detail or specifics about the type of scam Mr K was falling victim to. Having links that direct customers away from the payments page of a website are unlikely to have much effect on them proceeding with payment. And so Mr K was left without any insight into what he might be on the lookout for. The type of scam he fell victim to wasn't brought to life for him.

My finding is then that Moneycorp fairly and reasonably could have and should have questioned what Mr K was doing and that the loss could have been avoided as a result.

Did Mr K act reasonably in the circumstances?

I know that Mr K had no idea he was falling victim to a scam. He of course wouldn't have made the payment if he had. However, I do find there were sufficient indicators that all was not as it seemed here. To the extent that I believe Mr K ought to have investigated further, and where the scam would more likely than not have been revealed.

I've considered the price offered for the villa. After negotiation this was set at EUR10,850 plus EUR884 for servicing and a further EUR545.60 for tax. This was for a month's accommodation. Having looked into this I can't see that was a price that could be trusted; it looks too good to be true.

I know Mr K has said he carried out research and found other properties at a similar price. I've not seen any evidence of that, though I wouldn't really have expected Mr K to keep hold of such information at the time.

But, looking now, it seems impossible to find a broadly similar villa – in terms of size, location, and standard – for that price. Everything is significantly more expensive, even perhaps allowing for some inflationary adjustment. And I note that the scammer accepted a significantly reduced price from that originally advertised. Whilst that could, in part, be explained by benefitting from an extended booking discount. It doesn't seem plausible to me that such a discount would be agreed on a premium property, at an in-demand location, during peak holiday season.

Finding a booking for the length of time requested is also difficult, even though I am searching now (in February) for the same period Mr K was looking for (July), where he was looking toward the end of April. So I'm satisfied the offering ought to have been viewed with suspicion.

There is then the fact the supposed host wanted to take communication and booking away from the official website. Mr K even questioned this at the time, asking if it would be an entirely private or agency reservation. Clearly this meant that any protection that might have been offered by the site was foregone.

Mr K contacted a specific email address when enquiring about the booking. But he seems to have received a response from someone completely different, using a different email address. I can't see this was ever questioned and there was no establishing of who the parties involved were.

When it did come to booking, the process was then to be switched to a sister company of the original UK website. But there was little to establish a link between all the parties involved. And there appears to have never been the involvement of any booking portal. Whilst I can see the emails sent to Mr K, supposedly from the sister website, were well put together forgeries, I still believe the wider circumstances ought to have given rise to concern. There was no verifying of the source of those emails.

It's also true that Mr K was clearly being instructed to pay an individual where he believed he was transacting with a business. I've already said how Moneycorp ought to have identified this. But I find it's fair and reasonable to say Mr K ought to have too. This finding is strengthened further by the fact that the first set of account details he was given were also in an individual's name, and that they didn't work.

Those two personal accounts were clearly based in Spain. But Mr K had been told he'd be dealing with the French version of the UK website. Whilst both countries are European, it's another inconsistency that doesn't add up.

I'm satisfied these factors combined mean Mr K ought fairly and reasonably have realised something was amiss. The level of checks carried out then were not proportionate to the risk in the circumstances. Referring back to the original website, or doing some extra digging, would more likely than not have revealed the scam. And so, on that basis, I believe it would be fair and reasonable for him to hold some responsibility for the loss

Putting things right

The award I intend to make is as follows:

- A refund of 50% of the funds lost to the scam

- *Payment on that refund at 8% simple per year, calculated from the date of loss to the date of settlement.*

My provisional decision

I uphold this complaint against TTT Moneycorp Ltd.

Ben Murray
Ombudsman