DRN-5895716

The complaint

Mr M complains that Lloyds Bank PLC ('Lloyds') won't refund the money he lost to an investment scam.

He's represented by a firm of solicitors. For simplicity, I'll refer to Mr M throughout this decision.

What happened

The background is known to both parties, so I won't repeat all the details.

In summary, Mr M says that, in May 2024, he received a message from an individual ('K'). K presented as a business owner from abroad, involved in the fashion industry, looking to expand his business. Mr M was led to believe K was seeking friendship to help him navigate the UK market. A short time after, Mr M was also put into contact with another individual ('S') claiming to be K's girlfriend. He later discovered he'd connected with scammers.

A relationship started to develop and Mr M was soon persuaded to invest in cryptocurrency. He was provided with a link to open an 'account' with a crypto-platform ('B'), which seems to have been set up as a clone of a legitimate crypto-exchange. Mr M says things appeared to be going well at first, with his money doubling after a few trades. However, each time he later attempted to withdraw his funds, he was told he needed to pay more for that to happen.

Between May and August 2024, Mr M sent about £30,000 from his Lloyds account for 'investment'. The majority was sent through his accounts with genuine crypto-exchanges before being sent on to the scammers' wallets from there. But two payments were instead sent directly to the personal bank account of an individual ('X'). Mr M says he was told X was an investor and friend of the scammers (K and S), who'd deposit those funds on his behalf.

I've listed below the payments Mr M complained about. To note, payments 12 and 13 were not included in his initial list but were considered by Lloyds as part of its investigation.

	Date	Method	Payee	Amount
1	25-May-24	Card payment	Mr M's crypto-platform	£500
2	27-May-24	Card payment	Mr M's crypto-platform	£2,000
3	28-May-24	Faster payment	X	£2,000
4	28-May-24	Card payment	Mr M's crypto-platform	£2,700
5	28-May-24	Card payment	Mr M's crypto-platform	£400
6	31-May-24	Faster payment	X	£4,860
7	02-Jun-24	Faster payment	Mr M's crypto-platform	£5,000
8	22-Jun-24	Faster payment	Mr M's crypto-platform	£100
9	22-Jun-24	Faster payment	Mr M's crypto-platform	£3,000
10	26-Jun-24	Faster payment	Mr M's crypto-platform	£1,800
11	26-Jun-24	Faster payment	Mr M's crypto-platform	£2,500
12	01-Jul-24	Faster payment	Mr M's crypto-platform	£5,100

13	18-Aug-24	Card payment	Mr M's crypto-platform	£100

A complaint was made to Lloyds in January 2025 and later referred to our Service. Our Investigator considered it and didn't uphold it. In brief, although she thought the payments to X were covered by the Contingent Reimbursement Model ('CRM') Code, she wasn't persuaded Mr M had a reasonable basis for belief when making them. She was satisfied Lloyds had fairly established this exception to full reimbursement. And although she thought Lloyds ought to have provided Mr M with an effective warning on his second payment to X, she wasn't persuaded such a warning would have made a difference to what happened.

Outside of the CRM Code, she wasn't persuaded proportionate steps from Lloyds could have prevented the scam, given how Mr M responded when it did intervene. She was satisfied Mr M had been given the opportunity to explain what he was involved in, but didn't. And, on balance, she didn't think an earlier intervention would have made a difference either.

As the matter couldn't be resolved informally, it's been passed to me to decide.

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. These are the key reasons for my decision.

In broad terms, the starting position in law is that a firm (like Lloyds) is expected to process their customers' authorised payment instructions without undue delay. It's not in dispute that the payments in question were authorised. This means Mr M is presumed liable for them in the first instance. However, because Mr M says the payments were made as a result of him falling victim to a scam, there are some further considerations that may be relevant to whether it would be fair to expect Lloyds to refund the money he lost.

The CRM Code

Lloyds was a signatory to the CRM Code. This was a voluntary code which required firms to reimburse customers who have been the victims of APP scams in all but a limited number of circumstances. The CRM Code only applied to authorised push payments (such as faster payments) made between two accounts, denominated in pounds sterling, in the UK. For the CRM Code to apply, the payment also had to be made to an account of another person.

So the CRM Code doesn't apply to payments Mr M made by card or to his accounts under his control. But Mr M made two transfers to an individual X. He says this was someone he understood was a friend of the scammers, who would deposit the funds on his behalf. So, the Code could apply to payments 3 and 6 above, assuming that X was linked and also part of the scam. It's not entirely clear, from the evidence, whether X was involved in perpetrating the scam, or was also a victim, or simply provided cryptocurrency in exchange for Mr M's funds. However, Lloyds hasn't argued the provisions of the CRM Code shouldn't apply to those specific payments – so I've also proceeded on that basis.

A firm may still choose, under the CRM Code, not to reimburse a customer if it can establish that:

The customer made payments without having a reasonable basis for believing that:

- the payee was the person the customer was expecting to pay;
- the payment was for genuine goods or services; and/or

- the person or business with whom they transacted was legitimate.

The customer ignored what the CRM Code refers to as an 'effective warning' by failing to take appropriate action in response to such an effective warning.

**Further exceptions outlined in the CRM Code don't apply to this case.*

It's for Lloyds to establish if exceptions to reimbursement apply. Here, it has said Mr M didn't have a reasonable basis for belief when he paid X as he completed no checks and took everything he was told by the scammers at face value. And, again on the basis that Mr M's payments to X are considered to be covered by the CRM Code, I'm satisfied one of the listed exemptions to reimbursement under those provisions applies. I'm not persuaded Mr M had a reasonable basis for believing that the person he transacted with was legitimate.

I can accept there may have been some relatively sophisticated aspects to the scam, including the use of a clone and a convincing trading-platform. I can also accept Mr M thought he could trust the people he was dealing with. At the same time, the link he was given to B, clearly didn't match that of the legitimate exchange. I've seen little to suggest Mr M questioned or was given a plausible explanation as to why that was. And I can't overlook Mr M started to send significant amounts for 'investment' on the advice of individuals, in the "fashion industry", he'd only met through unsolicited contact just over a week earlier.

I've not been provided with any of the messages Mr M exchanged with K and S. And apart from Mr M's comments that he watched 'tutorial videos' about the genuine crypto-exchange and that he believed in K and S's explanations, I've been provided with little other evidence to show what he was told or how that relationship developed, such that I might be persuaded it was reasonable for him to believe he was dealing with genuine/professional individuals.

In his submissions, Mr M has also told us he was promised a rate of return of 30%. He hasn't specified over what period. But he's said the *"high returns and immediate results created the impression of minimal risk"* and that he *"watched his money double after a few trades".* In my view, these kinds of returns would strike most people as 'too good to be true' and should have signalled something was wrong, even to an inexperienced investor.

While Mr M has also said the scammers justified the high returns/minimal risks by reference to *"unique"* investments *"backed by advanced trading strategies and market insights",* I've again seen little to persuade me he was given plausible information around that or that he carried out sufficient checks independently of the scammers (as would reasonably be expected) into what he was being told or how those returns could realistically be achieved.

In relation to X's role in receiving his money, Mr M has told us the scammers explained that due to complications in him sending funds directly to his account with the crypto-exchanges, he had to deposit through X. But he's also said he *"didn't ask for or receive evidence that X was genuine or that X would deposit his funds in crypto"*. To me, it seems he paid someone he knew nothing about other than what the scammers had said about X being a friend and another investor. And, by virtue of what I've said about Mr M's relationship with K and S, including how that contact came about and the apparent lack of sufficient checks into the information he was given, I'm not satisfied he had a reasonable basis of belief that he was transacting with a legitimate person when making payments to X.

As such, I'm satisfied Lloyds can rely on this exception and isn't required to reimburse Mr M's payments to X in full, under the provisions of the CRM Code.

Lloyds' obligations under the CRM code

Even though I'm not persuaded Mr M had a reasonable basis for belief when making his payment to X, he may still be entitled to a partial refund of those lost funds if Lloyds didn't meet its obligations under the CRM Code – one of which is to provide effective warnings.

The CRM Code says that, where firms identify scam risks, they should provide effective warnings to their customers. And, looking at the account activity, I think Lloyds should arguably have provided Mr M with an effective warning, as required under the Code, when he made his second (not the first) payment to X. This was the second payment to a relatively new payee and of significant value. But under the CRM Code, the assessment of whether a firm has met a standard or not, should involve consideration of whether compliance with that standard would have had a material effect on preventing the APP scam that took place.

As referred to by the Investigator, Lloyds did identify a risk on a number of Mr M's payments. It spoke to him to find out more on several occasions. As I'll explain more below, Mr M didn't disclose anything significant about what he was really involved in and moved past warnings on crypto-investment scams. He's also said he genuinely thought that disclosing too much [to his bank] might result in unnecessary scrutiny or delays; that he believed in the narrative *"about banks being hostile to crypto";* and that he didn't explain things fully when questioned because he thought Lloyds was only trying to discourage him from investing. He's told us he didn't *"see the warnings as serious at the time"* and that *"when I was warned about crypto-currency scams, I honestly couldn't see it applying to me"*.

I'm not convinced Mr M would likely have been honest about what was going on, such that Lloyds would necessarily have been in the position to provide an effective warning. And, on his evidence, I don't think I can reasonably find Mr M would have likely reacted positively to an effective warning, if Lloyds had given him one when he made his second payment to X, such that I can reasonably find it should provide a partial refund of that money.

Prevention

The regulatory landscape and good industry practice sets out requirements, outside of the CRM Code, for firms to monitor accounts and have systems in place to look out for unusual transactions which might indicate its customers are at risk of financial harm from fraud. I'd expect Lloyds to take additional steps before processing payments in some circumstances.

But, as noted above, Lloyds did identify a possible risk on a number of Mr M's payments. It spoke to him on several occasions to find out more about what was happening.

In a call, on 2 June 2024, in relation to a blocked payment for £5,000, Mr M was asked for the payment reason. He responded he was investing in cryptocurrency and that he was sending the money to his crypto-exchange. He was warned of scammers posing as brokers and guiding victims to transfer their money for investment. At the end of the call, when asked if anyone had contacted him or told him to move his money for any other reasons, he replied *"no, not at all"*, that he was investing for himself, and putting into practice what he'd learned.

Two payment blocks were discussed during an intervention call on 8 June 2024. Mr M was told, at the outset, that the questions were to prevent a possible scam. For the earlier payment he'd attempted, on 4 June 2024, he confirmed he was sending funds to buy cryptocurrency from a crypto-account only he could access. When asked if he'd received advice from anyone, such as an adviser, broker, friend or family, Mr M responded *"not at all".* He said he was learning to trade. When again asked if he was taking advice, he said he took a *"course".* He was warned of scam victims taking advice from people they'd met on social media. He was warned that trading in cryptocurrency was high risk, to take advice only from accredited advisers, and to trade only on his own account, not through somebody else.

When asked if anyone had advised or asked him to download *apps* or click on any links, Mr M again responded *"no, not at all".* To add, I'd also note that when asked about the second payment he was sending that day to his account with another bank ('O'), he said he needed it when travelling abroad to his home country. Looking at Mr M's account with O, I can't see that this money was used for spending while travelling. And I'm aware he's also complained separately about payments from O being used to fund the scam.

In another intervention call, on 22 June 2024, Mr M was asked to be open, answer honestly, and not to hold back, so the bank could best protect him. Mr M said he understood. But when asked how long he'd been involved in cryptocurrency, he replied he'd taken *"courses"* and had been investing *"by myself"* for about a month. When probed, he said the 'courses' were through an online college and about investments in general. When asked if he'd been shown/given instructions about what to invest in, he replied *"no, it's just general information"*. He confirmed he'd not been approached/discussed any types of investment or been contacted through calls, emails, text or social media. There was no-one giving him any type of instructions. Despite being warned about common crypto-investment scams and social engineering, and that it's not true banks dislike cryptocurrency, he again confirmed he'd not been contacted by anyone and that he was happy for the payment to be made.

I'm mindful of Mr M's comments that his responses *"weren't intentionally dishonest".* But I can't fairly say that the scam wasn't unravelled as a result of a failure on Lloyds' part when it stepped in. It's clear that, despite relevant warnings, Mr M wasn't going to reveal anything significant about what he was really involved in. On the evidence, I'm not persuaded the losses would have been prevented even if Lloyds had probed/intervened more often than it did. And, while I recognise the importance of timely interventions, Mr M has told us that *"at no point was I given guidance on how to respond to the bank".* Further, *"every decision I made, every response I gave, was based solely on my own understanding and the trust I placed in [the scammer]. I acted in good faith, independently and without external influence."*

To me, that's questionable. But, if I take what Mr M has said were his pre-conceived ideas about the relationship between banks and cryptocurrency at face value, and considering also the little evidence to show his communication with the scammers at the relevant time, I'm not convinced I can reasonably conclude an earlier intervention would have played out very differently to the ones I've set out above. So, while I'm very sorry Mr M was the victim of a scam that's affected him deeply, I don't think it'd be fair and reasonable to hold Lloyds liable for his losses in circumstances where I think it's unlikely it could have prevented them.

Recovery

A bank is generally expected to attempt recovery once a scam has been reported. For the payments to X, it's unlikely funds remained to be recovered by that time. For the transfers to Mr M's accounts with crypto-platforms, he would have been able to access them himself if any remained. For the card payments, it's unlikely a chargeback would have succeeded given there's no dispute the cryptocurrency was provided before it was sent to the scam.

My final decision

For the reasons I've given, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 5 February 2026.

Thomas Cardia
Ombudsman