DRN-3764216

The complaint

Mr M complains that Ulster Bank Ltd won't refund money he lost as a result of a scam.

What happened

On 4 October 2022 I issued my provisional decision on this complaint. I gave both parties an opportunity to respond with further information before I issued my final decision. That provisional decision forms part of this final decision and is copied below.

What happened

Mr M had an interest in cryptocurrency. In mid-2019 he was contacted by someone claiming to represent an investment company. Unfortunately for Mr M, he was actually dealing with fraudsters.

Mr M decided to invest and, in order to fund his investment, he was instructed to make card payments to well-known money remittance services. Over the following months the amounts of the payments increased, and Mr M sent faster payments from his online banking to a variety of different recipients. It is not entirely clear whether the initial card payments went to the same recipient and are part of the same scam as the later faster payments, but Mr M has only disputed two of the card payments he made.

At first, Mr M's investment appeared to be doing well and he even received a sum back from the fraudsters. He could see the investment's performance through a trading platform which he was given access to. Later the fraudster told Mr M that if he invested £50,000, he'd receive the same amount back and £50,000 worth of cryptocurrency in just one week. Mr M borrowed money from a relative to continue investing but, at the end of the week, his 'account manager' said he'd need to pay money in order to withdraw his investment. And, after Mr M made a final payment, the account manager called him to say that they'd been arrested. At this point, Mr M realised he'd been the victim of a scam. In total Mr M says he lost £78,670. He also persuaded other family members to get involved in the scheme and, unfortunately, they also lost money.

The faster payments Mr M made went to a number of other financial or cryptocurrency related businesses. Mr M says he gave remote access to his computer to the representative of the investment company and they guided him through much of the process of converting his money into cryptocurrency and sending it to the trading platform. He also says that, on occasion, the fraudsters would carry out transactions themselves, without any involvement from him.

The payments Mr M disputes are set out below:

Payment number	*Date*	*Amount*	*Payee*
1	*26 August 2019*	*£1,585*	*1 (card payment)*
2	*3 September 2019*	*£1,585*	*1 (card payment)*
3	*11 September 2019*	*£5,500*	*2*
	23 September 2019	*£49,994 (credit)*	

4	*24 September 2019*	*£20,000*	*3*
5	*25 September 2019*	*£10,000*	*4*
6	*25 September 2019*	*£10,000*	*5*
7	*26 September 2019*	*£10,000*	*5*
	15 October 2019	*17,994 (credit)*	
8	*15 October 2019*	*£20,000*	*6 (Mr M's relative)*

His account at Ulster Bank had only been opened a month before he sent the first disputed payment and, I understand, the only debits that took place on it were related to the fraud. After a review of the account, Ulster Bank decided to close Mr M's account and it did so in March 2020.

In May 2020, after several months of trying to reach the fraudster and recover his funds, Mr M complained to Ulster Bank about falling victim to a scam. It said that he had willingly made the payments and its attempts to recover his money had been unsuccessful – so it wasn't going to provide a refund.

It also questioned whether it could be held responsible for the loss at all, as none of the payments Mr M made appear to have gone directly to the fraudulent investment company. Instead, the payments went through several intermediaries.

Mr M referred the matter to our service and one of our investigators upheld his complaint. They argued that Ulster Bank ought to have found almost all of the activity on Mr M's account to be unusual and suspicious given the significant sums involved and the fact the payments went to various cryptocurrency providers. So, in their view, it should have intervened when Mr M made the first faster payment from his account of £5,500 and, had it done so, the scam would have been prevented. They noted that the account had been closed because Ulster Bank had concerns about the way it was being operated, albeit later than the disputed activity, and they thought Ulster Bank should have shown concern earlier.

They also didn't think it would be fair for Mr M to take a share of the blame, given the sophisticated nature of the scam. So, the investigator recommended that Ulster Bank pay Mr M £75,500.

Ulster Bank disagreed, in summary it said:

- *It was satisfied Mr M had authorised all of the payments.*
- *It would be reasonable to expect Mr M to have conducted some research into the investment opportunity.*
- *It questioned whether an intervention would have made a difference if the fraudster had control of Mr M's accounts.*
- *It disputes that payments to cryptocurrency providers are necessarily higher risk than any others and argues that the vast majority of such payments are legitimate.*
- *It denies that its later concerns about the way the account was being run meant it should have recognised Mr M was at risk of financial harm from fraud at the time the*

  payments were made.
- *While it follows good industry practice, it did not have any concerns about the activity which took place on Mr M's account. It would not be practical, nor is it a*

useful indicator of fraud, to simply block all high value payments.

- *It questioned whether there is any evidence that a verbal conversation is more effective at preventing scams than a written warning.*
- *It would never have been able to recover the funds as they went to cryptocurrency accounts in Mr M's name.*

As no agreement could be reached, the case was passed to me for 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.

I've first considered authorisation. The starting position, under the Payment Services Regulations 2017 and the terms of Mr M's account, is that he is responsible for transactions he has authorised.

Given that the fraudsters, at times, had control of Mr M's computer, there's some uncertainty about whether he authorised each and every transaction from his bank account. But, even if Mr M didn't actually carry out each transaction, it's evident that he either consented to them taking place or consented to the third party having control of his accounts given that, at the time, he was willingly investing his money into the scheme. Mr M says he did not share his online banking security information so that a third party could access his account without him being present. So, I'm satisfied the disputed transactions were authorised and I've gone onto consider whether there is any other reason for Ulster Bank to refund Mr M.

The Lending Standards Board Contingent Reimbursement Model "CRM Code" requires its signatories to reimburse victims of APP scams like this one in all but a limited number of circumstances. However, having considered this matter carefully, it seems to me that the CRM Code does not apply to the payments Mr M made. Though, it's important to note, it's not exactly clear what happened to each and every payment, so I've reached this finding on the balance of probabilities.

In total Mr M disputes eight different payments, which went to six different beneficiaries. I've considered each payment in turn.

For the provisions of the CRM Code to apply, a payment must (among other less relevant conditions):

- *Be a faster payment, CHAPS payment or payment between two accounts at the same bank that would otherwise be a faster payment.*
- *Be sent to another person.*
- *Be between pound sterling denominated accounts in the U.K.*

The first and second payments are card payments and therefore not covered under the CRM Code. As the payments were to a genuine business which will have carried out a service for Mr M (the transfer of money), there would have been no grounds for Ulster Bank to challenge the payments through the chargeback scheme either.

It appears that payments three and four went to two different cryptocurrency trading businesses, but not ones that allow a customer to operate an account which holds electronic money or cryptocurrency. Instead, they seem to offer simple exchange functionality. It's likely therefore that Mr M (or the fraudster on his behalf) simply

purchased cryptocurrency and instructed the respective businesses to send it to a cryptocurrency wallet they had control over. Assuming this is correct, I do not consider these payments to be caught by the CRM Code. That's because although the payment from Mr M's bank account to the cryptocurrency exchange meets the definition above, the payment from the cryptocurrency exchange to the cryptocurrency wallet, does not. That payment was a payment in cryptocurrency, not pound sterling.

I've reviewed evidence that the fifth payment went to an account in Mr M's name. He says he didn't set up or have access to this account. But I'm not entirely convinced by this. The business which provided the account say it was set up in June 2019 – several months before Mr M made the £10,000 deposit to the account. That business says that Mr M even contacted it to query a £2 deposit in early July 2019 and that the device used for all the activity (including the disputed activity) is the same. I also note Mr M's comments about allowing a third party to access his device during some of the activity. The fact his device appears to have remained the same before and after the disputed activity would be consistent with this account of events. Overall, it seems more likely than not that this was an account that Mr M set up and it can fairly be considered as his own account. As such, the CRM Code does not apply to the fifth transaction as the payment didn't go to another person.

There isn't the same evidence around payments six and seven, but they do go to a business which appears to offer both a pure exchange service (like the recipients of payments three and four) and the provision of a cryptocurrency account. In either case I don't think the payments are covered by the CRM Code, as it's more likely than not that Mr M's money would have been received by the fraudster in cryptocurrency, not pound sterling.

The final payment went to a relative of Mr M. She was also a victim of the same fraud. It appears that this money went from Mr M's relative's account to the same payee as payment three (or, at least, a business offering very similar services) and was sent there with his agreement. I'm satisfied this payment formed part of the scam that Mr M fell victim to.

However, I don't think this payment is covered by the CRM Code either – though the transaction from Mr M's account to his relative and the relative's subsequent payment to the cryptocurrency exchange do satisfy the conditions of the CRM Code, the final payment from the cryptocurrency exchange to the fraudster does not – it was a payment in cryptocurrency not pound sterling.

So, I'm satisfied that the CRM doesn't apply here. However, taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Ulster Bank should fairly and reasonably:

- *Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.*
- *Have had systems in place to look out 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 payment service providers are generally more familiar with than the average customer.*
- *In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases decline to make a payment altogether, to help protect customers*

from the

possibility of financial harm from fraud.

This was a new account, opened largely, if not exclusively, for the purpose of investing in what turned out to be a fraudulent scheme. As such, there's little genuine account activity to compare the fraudulent payments against. In fact, apart from credits to the account, the spending is only fraud related. It begins with payments to money remittance services and ends with a series of faster payments to various different financial or cryptocurrency related businesses.

So, I'm mindful that Ulster Bank would not have had any meaningful previous account activity to compare the spending against and I've taken this into account when deciding whether it should have found the activity suspicious. Nevertheless, I think, by a certain point, the way in which the account was being used ought to have concerned Ulster Bank.

The only activity on the account prior to the payments in dispute were payments to money remittance firms. I wouldn't have expected Ulster Bank to have questioned Mr M about these payments – they were of a relatively modest value. And, though Mr M only appears to be disputing the two most recent payments of this type, my view would be the same if he disputed the earlier ones too. Though I don't think this activity was suspicious enough for Ulster Bank to be concerned, I suspect that the activity of opening an account only to use it to make this kind of payment is quite unusual. What followed was a significant credit to the account and a series of high value payments to various different payees.

Ulster Bank argues that it isn't fair to point to its later concerns about how the account was being used as evidence that it did, or should have had, concerns about the account at the time. I accept that its later decision to close his account was made for other reasons. But, that doesn't mean it shouldn't have considered whether Mr M was at risk of financial harm from fraud when the payments were being made.

I also don't dispute that there are many legitimate payments made to cryptocurrency providers, but Ulster Bank would have been aware of the risks of cryptocurrency scams since at least January 2019, including their common features. It's not clear whether Ulster Bank did know where all of these payments were going (as I've set out above – it's been quite difficult for me to establish), but I certainly can't agree that if it did, this should have provided it with reassurance.

Taking all of the above into account, though I do think Ulster Bank should have intervened here, I've reached a different finding to that of the investigator about when that intervention should have taken place. I don't think, given the very limited account history, that Ulster Bank could have reasonably suspected fraud in relation to the £5,500 payment. Neither, I think, should it have stopped the £20,000 or first £10,000 payment. While they were clearly significant amounts, I don't think their size alone makes them sufficiently remarkable, taking into account the fact that Ulster Bank wouldn't have had much of a picture of what was unusual for Mr M. However, by the time the second £10,000 payment was attempted it should have been clear to Ulster Bank that the account wasn't being used in a typical fashion. There were no regular credits or debits to the account and the large credit of almost £50,000 was being removed from the account in a series of relatively rapid payments.

So, despite the fact that Ulster Bank could not have a good understanding of what Mr M's typical account usage was, I think that when he made the second £10,000 payment a concerning enough pattern had developed that it ought to have intervened. While its

concerns might not have been solely about whether Mr M was at risk of financial harm from fraud, a conversation would have quickly established that there was risk to him.

Ulster Bank says it provided a written warning to Mr M before he made each payment, but I don't think that was enough of an intervention in the circumstances. Also, from its records, it's not entirely clear which warning it gave. Customers were required to choose a payment reason for each payment, but I can't see from Ulster Bank's records which payment reason Mr M chose. But, even if Mr M did choose 'investment' and was provided with the warning tailored to investments, I don't think this was sufficient in the circumstances. It wasn't tailored to the specific risk of cryptocurrency scams and didn't highlight any of the common features. So, I think Ulster Bank ought to have done more and contacted Mr M about the second £10,000 transaction. Inevitably it's very difficult to know what would have happened had Mr M been contacted at the time and asked a few questions about the activity he was carrying out. But I think it's likely that he would have revealed:

- *His lack of understanding of exactly where the transactions were going and for what purpose.*
- *He was being directed to make the payments by a third party who had, at points, taken control of his computer.*
- *He'd also made payments to a third party via a money remittance service.*
- *He'd been promised an instant 100% return, if he invested £50,000.*
- *He'd been encouraged to borrow money in order to keep investing.*
- *He was dealing with an unregulated investment company.*

Even if only some of the above was revealed by Mr M, I think it should have given Ulster Bank significant cause for concern and would have put them in a position to give a very strong warning to Mr M that he was falling victim to a scam.

I'm mindful that Mr M had already invested a significant sum at this point, but I've not seen any compelling evidence that he would have carried on regardless of any warning provided by the bank. In any case, I think that a conversation would have likely caused Ulster Bank so much concern that it may have had reasonable grounds to prevent Mr M from carrying out further transactions.

I can't agree that such an intervention would have been any less effective because the fraudsters may have been in control of Mr M's computer at the time the payment was made. Ulster Bank would have spoken to Mr M, not the fraudsters and it would have been able to take all necessary steps to secure his online banking.

So, I think Ulster Bank's failure to pick up on the unusual activity has caused Mr M loss.

I've also thought about the role Mr M had to play in what happened. There were clearly relatively sophisticated elements of this scam – including the provision of a trading account that appeared to show the status of his investment. I'm also conscious that Mr M has little investment experience and I think he, as well as someone with his knowledge and experience, would be less able to pick up on the concerning aspects of what unfolded. I've also seen some paperwork, including in relation to the supposed £100,000 that Mr M was due to receive, and it appears relatively convincing.

However, there are aspects of what happened which I think should have concerned Mr M. I understand he was told that the fraudulent investment company were running a promotion which would mean for a £50,000 investment, he would receive £100,000 back

in just a week. While I understand he could see this amount in his account at the trading platform, it's not clear that Mr M questioned how or why the fraudulent investment company would give him this money and, I'm afraid, such an offer seems to be good to be true.

It's also clear that Mr M, rather than asking for his £100,000 back at the end of that week, instead invested more money. It also appears Mr M may have been told he needed to invest more money to get back his profits. I think these factors should have been significant red flags for Mr M and, though I understand he's likely to have been put under a lot of pressure by the fraudsters, I don't think it was reasonable for him to keep making payments.

So, I think that by the time he made the second £10,000 payment, he'd been presented with an offer that was simply too good to be true. That means I think that a deduction of 50% should be made from the refund Mr M receives.

To be clear, while I know this will be very disappointing for Mr M, I am recommending that Ulster Bank pay him 50% of payments 6 and 7 – a total of £10,000. I've excluded the final payment because it was sent to Mr M's relative and has already been considered as part of a separate complaint. In relation to interest, I understand the money used for these transactions was borrowed from a family member and Mr M was not charged interest on that loan. So, I don't award any interest.

I've also thought about whether Ulster Bank could have recovered Mr M's funds, but I don't think this would be possible. Mr M's money was either sent directly to the fraudster and likely collected in cash (as in the case of the money remittance transactions) or sent to an intermediary before being exchanged into cryptocurrency and sent to the fraudster (in the case of the other transactions). It follows that we know that the businesses involved don't hold Mr M's money and neither Ulster Bank nor the intermediaries would have any way of recovering it.

Finally, I thought about compensation. While I recognise the significant impact being without this money has had on Mr M, I have not found that the bank is fully, or even mostly, responsible for his loss. That also means that I cannot say the majority of the distress and inconvenience is the fault of the bank either. Taking this into account, I think Ulster Bank should pay £100 to Mr M to recognise the role it's had in what happened.

My provisional decision

I intend to uphold in part this complaint about Ulster Bank Ltd and ask it to pay Mr M:

- *£10,000*
- *£100 compensation*

Ulster Bank accepted my provisional decision. Mr M did not. He explained that the outcome would be devastating for him and his family. In summary, he also argued:

- The fraudster used sophisticated techniques to initially entice him and then keep him depositing more funds. He was first given the impression that there was no risk, but later he was told he had to keep depositing more money to save his investment.
- Had Ulster Bank contacted him during the fraud he wouldn't have gone ahead with the payments, but there's no evidence the bank did this or provided any warnings to him. He'd like proof that warnings were displayed.

- The first large payment of £5,000 should have been the point at which it intervened.
- Ulster Bank made no attempt to recover his funds.
- The CRM Code is applicable here and it says firms should refund customers, like him, who were vulnerable to fraud.
- The bank ought to have challenged the payments through the chargeback scheme.
- The Banking Protocol hasn't been considered.
- My provisional decision isn't consistent with other decisions issued by our service, several examples of which he has provided. Neither is it consistent with case studies published on our website.

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 to hear of the devastating impact this matter has had, and is having on, Mr M. I don't wish to cause him any further distress – but I must give my decision based on what I consider to be fair and reasonable, taking into account all of the evidence.

I've considered Mr M's submissions carefully, but I'm not persuaded to reach a different outcome to my provisional decision. I'll explain why.

I set out in my provisional decision why the CRM Code does not apply to any of the payments made. Though Mr M has argued that his position would be different under the CRM Code, he hasn't provided any arguments as to why that code applies. I'm satisfied it doesn't for the reasons I've already outlined, so I won't comment on this further.

In addition, the Banking Protocol only applies to payments made in branch. Similarly, the chargeback scheme only applies to card payments and I've already explained why a chargeback wouldn't be successful for the two card payments in dispute. In relation to the recovery of funds, I've already set out why I don't think this would have been possible in the circumstances.

I agree that the bank had obligations to be on the lookout for unusual and out of character transactions. I've explained that I think it failed in those obligations and should have intervened before allowing some of the payments to proceed. I've also explained that I think that a conversation with Mr M would have made a difference to his decision to keep investing and prevented any further loss to him. And, I've also set out that there's no clear evidence any warnings were provided, but, even if they were, I don't think this would have been sufficient in the circumstances. So, much of what Mr M argues isn't really in dispute.

I think there are only two remaining points of actual disagreement that I can comment further on: the point at which Ulster Bank should have intervened and whether Mr M should bear any responsibility for the loss.

I've already explained why I think the intervention should have taken place when it did and not earlier. I've had to carefully balance the fact that Ulster Bank had no meaningful account activity to compare the fraudulent transactions against with the fact that the value and frequency of the payments should have given it cause for concern. I'm afraid there's little more that I can add to this point. I cannot comment on other decisions issued by our service and I've decided this case on its own merits.

Finally, I do accept the sophisticated aspects of the fraud and the pressure that Mr M was put under. I accept that he had little investment experience and that this fact was exploited

by the fraudsters. Nevertheless, I cannot agree that it was reasonable for him to believe that his money would be doubled, seemingly without any risk, in just a week. So, I continue to be of the view that a 50% deduction is fair.

I'm sorry to disappoint Mr M, but my final decision remains unchanged from my provisional findings.

My final decision

I uphold in part this complaint about Ulster Bank Ltd and instruct it to pay Mr M:

- £10,000
- £100 compensation

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 23 November 2022.

Rich Drury
Ombudsman