DRN-3734903

The complaint

Mr R says National Westminster Bank Plc ("NatWest"), didn't do enough to help when he fell victim to a an 'authorised push payment' ("APP") cryptocurrency investment scam. He says NatWest should reimburse him for the money he lost.

What happened

As both parties are familiar with the circumstances of this complaint, I've summarised them briefly below.

In summary, Mr R fell victim to a cryptocurrency investment scam. Mr R had some proceeds as a result of the sale of a property. He was duped into believing he was liaising with a genuine investment firm whom I'll call 'Company A'. Mr R made payments from his NatWest account to a cryptocurrency account in his own name, and then from there, on to Company A and an adviser that he thought would invest for him.

Mr R, seeing what he believed was successful trading and profit being made, made further payments, and also convinced three friends to sign up to trade with Company A. As Mr R had a cryptocurrency account already – his friends made faster payments into his account with NatWest, with Mr R then moving those payments on to his cryptocurrency account and then on to Company A, whom he thought was legitimately trading and investing on everyone's behalf.

Unfortunately Mr R had in fact cruelly been duped by fraudsters. Mr R uncovered that he had fallen victim to a scam when he and his friends were unable to withdraw any funds / profits. In total the following payments were made:

No.	*Date*	*Amount*	*To*	*Additional comments*
1	*21 October 2020*	*£10*	*Mr R's cryptocurrency account*	
2	*22 October 2020*	*£5*	*Mr R's cryptocurrency account*	
3	*26 October 2020*	*£800*	*Mr R's cryptocurrency account*	
4	*28 October 2020*	*£1,000*	*Mr R's cryptocurrency account*	*Intervention by NatWest*
5	*28 October 2020*	*£10*	*Mr R's cryptocurrency account*	
6	*29 October 2020*	*£7,000*	*Mr R's cryptocurrency account*	*Intervention by NatWest*
7	*29 October 2020*	*£8,000*	*Mr R's cryptocurrency account*	*Intervention by NatWest*
8	*30 October 2020*	*£10,000*	*Mr R's cryptocurrency account*	*Intervention by NatWest*
9	*30 October 2020*	*£9,999*	*Mr R's cryptocurrency account*	*Intervention by NatWest*
10	*10 November 2020*	*£5,000*	*Mr R's cryptocurrency account*	
11	*11 November 2020*	*£10,005*	*Mr R's cryptocurrency account*	*On behalf of Friend 1*
12	*24 November 2020*	*£9,999*	*Mr R's cryptocurrency account*	*On behalf of Friend 2*
13	*24 November 2020*	*£10,000*	*Mr R's cryptocurrency account*	*On behalf of Friend 3*

Mr R reported the matter to NatWest who ultimately didn't consider it was liable for the losses he incurred.

Unhappy, Mr R brought his complaint to our service.

Our Investigator didn't recommend the complaint be upheld. They explained that banks are expected to process payments and withdrawals that its customer authorises it to make. But they also explained that there are some situations where banks, taking into account relevant rules, codes and best practice standards, shouldn't have taken their customers' authorisation instruction at 'face value' – or it should have looked at the wider circumstances surrounding the transaction before making the payment.

In this case, the Investigator noted that NatWest intervened on the majority of the initial payments Mr R made to the cryptocurrency account that was in his name. They considered that NatWest's intervention arguably could have been better, and more questions asked of Mr R around the purpose for the payments. But in the particular circumstances of this case they didn't think it would have had a material effect on preventing the scam or losses. They considered that Mr R was under the spell of the scammer and had been advised by the scammer to tell the bank that he was buying cryptocurrency. So the Investigator wasn't persuaded that Mr R would have been forthcoming about Company A's involvement.

The Investigator also thought NatWest couldn't have prevented Mr R's losses had he gone into more detail about Company A. This was due to the sophistication of the scam – the company's website, positive reviews, that Mr R had received a contract and withdrawn some funds and there wasn't a warning on the Financial Conduct Authority's ('FCA') website about Company A until February 2021 which was after the payments Mr R made.

The Investigator also noted Mr R, during a call with NatWest, advised he was investing in cryptocurrency. NatWest advised that it didn't recommend he went ahead with the payment due to the amount of fraud it had reported to it in relation to cryptocurrency. As Mr R had a belief that everything was genuine, he confirmed he was happy to go ahead. So our Investigator thought, that on the whole, intervention wouldn't have made a difference in this case.

With regards to the recovery of any funds, as the funds had been sent to a cryptocurrency account in Mr R's name and had then been moved on from the cryptocurrency exchange provider there wasn't any funds that NatWest could recover.

Mr R disagreed with the Investigator's opinion and as the matter hasn't been resolved, 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.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

I'm very aware that I've summarised this complaint and the responses briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focussed on what I think is the heart of the matter here – which is to determine whether NatWest could have prevented Mr R's losses. If there's something I've not mentioned, it isn't because I've ignored it. I haven't. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as an alternative to the courts.

Having thought carefully about NatWest's actions, I'm not upholding Mr R's complaint. I do appreciate how disappointing this will be for him. Mr R was a victim of a sophisticated scam and has lost a significant sum which also involved close friends of Mr R losing funds. But in weighing everything up, so NatWest's actions and the testimony Mr R has provided about what happened, I don't think I can fairly say NatWest should reimburse him. I'll explain why.

Before I go on to explain my findings, I want to clarify for Mr R's benefit why the 'Contingent Reimbursement Model (often referred to as the 'CRM Code') isn't relevant in his case and what the relevant regulations were at the time.

Why the CRM Code isn't applicable

The CRM Code sets out under 'DS1(2) (a)' the scope of what the CRM Code covers in relation to authorised push payment ("APP") fraud. And that is instances where:

> *"(i) The Customer intended to transfer funds to another person, but was instead deceived into transferring the funds to a different person; or*
>
> *(ii) The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent."*

As the payments Mr R made from his NatWest account to the cryptocurrency exchange provider was to an account in his own name, it isn't covered by or within the scope of the CRM Code. This is because Mr R wasn't paying 'another person'.

The relevant law and regulations in place at the time

In broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the terms and conditions of the customer's account.

It is the case that Mr R authorised all of the payments and transfers that are in dispute – and that's accepted by all parties. And under the Payment Service Regulations 2017 (which are the relevant regulations in place here) that means Mr R is responsible for them.

That remains the case even though Mr R was the unfortunate victim of a scam.

But that isn't the end of the story, and 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 NatWest 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 banks 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 declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

What does this mean for Mr R?

Given the above, I've looked to see first, whether Mr R's transactions were unusual and out of character. And second, whether NatWest should have stepped in and intervened – so taking some additional steps or checks with Mr R about a payment. But importantly, I have to determine whether these additional checks or steps would have put NatWest on notice that something might not be right, and that Mr R may be at risk of financial harm or revealed the scam. In short, I have to consider whether any intervention by NatWest would have made a difference and prevented Mr R from making the payments – thereby preventing the loss.

Here, NatWest called Mr R in relation to the majority of the payments he made to his cryptocurrency account. Aside from a payment Mr R made for £5,000, on 10 November 2020 (Payment 10), and the three payments (Payments 11,12 and 13) that Mr R made on behalf of his friends, whom he had convinced to also invest.

Having listened to the calls, I agree with our Investigator in that there is an argument to say NatWest could have probed further than it did. It sought to satisfy itself that Mr R was aware of the payment(s) and sought confirmation of the destination account and how details for the account were obtained. It also sought the purpose for the payment. But I find there could have been more open and probing questions asked of Mr R here to satisfy itself that all was ok.

But, and importantly, despite any potential failings or shortcomings on NatWest's behalf – I have to consider whether intervention would have made a difference here overall. I have to weigh up what Mr R's belief was at the time he made the payments and take into account the narrative that he had been fed by the scammer about what to say to the bank when questioned and whether he would have proceeded with the payments in any event. This is the crux of the matter here.

Having looked through the messages between Mr R and the scammer, it is clear, that he was, unfortunately, well under the spell of the scammer. I am mindful that Mr R also conversed verbally with the scammer on multiple occasions, which I think more likely than not would have persuaded Mr R further and convinced him of the narrative he was being fed, which was to just say he was buying cryptocurrency and not to mention anything else. From listening to the calls it is clear Mr R was willing to stick to that narrative. And I find there to be, based on the balance of probabilities, a stronger argument that Mr R would have proceeded with the payments, and it is unlikely that he would have heeded any warnings or risks that NatWest might have put forward.

I have taken some extracts from the messages between Mr R and the scammer that supports this position.

[27/10/2020, 15:30:35] Mr R: Nice. Should be home at 5 yea.
[27/10/2020, 15:55:38] Scammer: great
[27/10/2020, 17:05:55] Mr R: Ready
[27/10/2020, 17:05:59] Scammer: kk
[27/10/2020, 17:28:07] Scammer: let me know when you've sorted it out
[27/10/2020, 17:29:56] Mr R: Was just on the phone but the line went dead
[27/10/2020, 17:30:06] Scammer: haha enjoy
[27/10/2020, 17:32:33] Scammer: try not to screw it up haha
[27/10/2020, 17:50:03] Scammer: got through?
[27/10/2020, 17:55:47] Mr R: [expletive].
[27/10/2020, 17:56:22] Mr R: They want me to go into branch and show them the [cryptocurrency] account with the proof of [bank] sort code and account number
[27/10/2020, 17:56:40] Scammer: okay amazing

[27/10/2020, 17:56:43] Scammer: can i call you
[27/10/2020, 17:56:49] Mr R: Yea

[28/10/2020, 15:39:09] Mr R: All done
[28/10/2020, 15:39:39] Scammer: nice bro
[28/10/2020, 15:39:45] Mr R: They said they may hold of future payments but they should go through
[28/10/2020, 15:40:03] Scammer: gotta love the banks
[28/10/2020, 17:25:12] Mr R: Sorry. Bank called me about the 7k [laughing emoji's]

[29/10/2020, 17:12:17] Mr R: What's the betting the bank will call me again [laughing emoji's]
[29/10/2020, 17:12:31] Scammer: probably
[29/10/2020, 17:12:43] Scammer: but at least they protect you
[29/10/2020, 17:12:53] Mr R: Yea true
[29/10/2020, 17:17:01] Mr R: It finally saved as a payee [hands up emojis]
[29/10/2020, 17:17:08] Mr R: My bank are going to call me shortly
[29/10/2020, 17:17:09] Mr R: [laughing emoji's]
[29/10/2020, 17:19:43] Scammer: amazing bro
[29/10/2020, 17:19:49] Scammer: just saying your buying bitcoin on [your cryptocurrency account]
[29/10/2020, 17:19:55] Scammer: you should be sweet
[29/10/2020, 17:20:37] Scammer: what bank you with
[29/10/2020, 17:27:01] Mr R: Yea exactly what I said.
[29/10/2020, 17:27:03] Mr R: NatWest
[29/10/2020, 17:27:20] Mr R: All approved waiting for [cryptocurrency provider] to confirm
[29/10/2020, 17:27:36] Scammer: amazing

[30/10/2020, 11:16:39] Mr R: 10k
[30/10/2020, 11:16:53] Scammer: oh sweet so you're fine?
[30/10/2020, 11:17:02] Scammer: it left your bank account?
[30/10/2020, 11:17:06] Mr R: Just need to ring the bank. Got a message
[30/10/2020, 11:17:13] Scammer: amazing bro lmk
[30/10/2020, 11:17:18] Scammer: trooper haha
[30/10/2020, 11:19:44] Mr R: Yea all good. Going through now.
[30/10/2020, 11:20:01] Scammer: lol so in 1 hour from now?
[30/10/2020, 11:20:06] Scammer: such [expletive]
[30/10/2020, 11:20:08] Mr R: Hopefully bro
[30/10/2020, 11:20:22] Mr R: [laughing emoji's]

[30/10/2020, 13:09:26] Mr R: On the phone to the bank
[30/10/2020, 13:09:48] Scammer: kk
[30/10/2020, 13:15:38] Scammer: all good?
[30/10/2020, 13:21:24] Mr R: Mission. That was a longer call [laughing emoji's]
[30/10/2020, 13:21:30] Mr R: Going through now

[11/11/2020, 07:16:12] Mr R: Morning mate. [Friend 1's] 10k hasn't come through so she is ringing the bank at 9am
[11/11/2020, 10:06:27] Mr R: She is hold with the bank at the Jp
[11/11/2020, 10:06:30] Mr R: Mo'
[11/11/2020, 10:06:40] Scammer: kk
[11/11/2020, 10:06:42] Scammer: lol
[11/11/2020, 10:06:43] Scammer: fun times
[11/11/2020, 10:06:45] Scammer: haha
[11/11/2020, 10:18:25] Mr R: Anything she needs to say if they ask what it's for v
[11/11/2020, 10:18:27] Mr R: ?'
[11/11/2020, 10:18:39] Scammer: just to send you money
[11/11/2020, 10:18:41] Scammer: nothing else
[11/11/2020, 10:18:54] Scammer: dont mention trading
[11/11/2020, 10:18:55] Scammer: lol
[11/11/2020, 10:18:56] Mr R: Ok cool
[11/11/2020, 10:19:02] Scammer: will make your life easier trust
[11/11/2020, 10:19:29] Mr R: Yea I bet [laughing emoji's]

[23/11/2020, 17:53:34] Mr R: Got the other one in too [strong arm emoji]
[23/11/2020, 17:54:19] Scammer: legend
[23/11/2020, 17:54:27] Scammer: the max they can do is 10k? correct?
[23/11/2020, 17:54:33] Mr R: I feel like a salesman [laughing emoji's]

[24/11/2020, 08:20:19] Mr R: Ma they had to speak to their banks so as soon as it it mine il send it to [cryptocurrency provider]
[24/11/2020, 08:28:29] Scammer: okay tell them they are just sending you the funds
[24/11/2020, 08:28:43] Scammer: try to leave out the trading part haha
[24/11/2020, 08:32:47] Mr R: Yea I already told them that [laughing emoji's]

In its initial call with Mr R, NatWest requested that he attend branch to provide identification and to also show the details of where the payment was going – which was a cryptocurrency account in Mr R's own name. Mr R attended branch the following day and NatWest released the payment. Given it was a new and recent payee, I find NatWest's intervention appropriate here.

With the subsequent calls I am mindful Mr R was advised to say he was just buying cryptocurrency and not stray from that narrative. He was also advised not to mention that it was for trading. Listening to the calls (while taking into account the conversations Mr R was having with the scammer about what to say) I think it was clear that Mr R intended to stick to that narrative and advised the bank that he had purchased some cryptocurrency, the account was in his name, and he was happy to proceed on each occasion.

There was an occasion where, as Mr R had said he was buying cryptocurrency, NatWest advised that it didn't recommend Mr R went ahead with the payment, due to the amount of fraud it had reported to it in relation to cryptocurrency. Mr R didn't heed the warning and confirmed he was happy to proceed. And unfortunately this seems to stem from Mr R's belief that everything was ok and the narrative he had unfortunately been fed by the scammer.

I am also mindful that Mr R was so convinced by things that he persuaded three other friends to join the venture, also advising them they should tell their respective banks, if talking to them, that they were sending him money and to not mention trading.

I note that NatWest didn't call Mr R on the later payments he made on behalf of his friends. But given the above, that Mr R had convinced his friends to invest, I think it is more likely than not, that he would have proceeded with the payments regardless of any intervention by NatWest.

I have given consideration to the fact that had NatWest probed further, would it have potentially made a difference. However, for reasons already explained I'm not so sure how much more information Mr R would have divulged, and I think it is more likely than not that he would have stuck to the purpose for the payments being for the purchase of cryptocurrency. I'm persuaded the conversations Mr R had with the scammer support that.

But even if some further questions had been asked, and if Mr R had shared some further information, I still feel Mr R would have been guarded on his responses. Even had he divulged that there was a company investing for him, which might have put NatWest on notice that Mr R may be at risk of falling victim to a crypto-investment scam, such was Mr R's belief in the scammer that I think Mr R would have proceeded in any event.

I also think it is more likely than not that if NatWest advised Mr R to make some additional checks, then Mr R would have been satisfied that things were ok. I say this because he had received what he thought was a contract, was persuaded by what he was seeing in terms of the website, his trading account and he had been able to withdraw funds. There also wasn't any adverse warning on the FCA's database at the time, a warning about Company A wasn't listed until February 2021 – which was after Mr R's payments.

I am also mindful that, given the rapport the scammer had built with Mr R, it is likely that Mr R would have reverted back to the scammer with any concerns. And I think the scammer would have appeased Mr R with a further narrative that the banks simply don't like risky trading. From what I've seen and on balance, I think Mr R would have accepted that narrative and continued. I say that as Mr R, possibly due to his belief in the scammer, appeared risk adverse and wasn't heeding any warnings from the bank. Rather it appears he considered the bank an obstacle when making his payments for himself and his friends.

Overall, based on the evidence I have seen, I'm not as persuaded as I would need to be to say that Mr R would have heeded any warnings or risks that NatWest might have put forward. So I can't fairly say that NatWest should be held liable for the losses Mr R incurred.

Recovery of the funds

Given Mr R sent the funds to an account he held in his name with a cryptocurrency exchange provider, which the scammers then helped Mr R move on under the guise of trading, there wasn't any funds that could be recovered from the cryptocurrency exchange provider by NatWest.

Summary

While I appreciate Mr R's been the unfortunate victim of a cruel scam, I think NatWest's decision not to refund him in this instance was fair and reasonable in the circumstances.

I say this because I'm satisfied the CRM Code isn't applicable to the payments Mr R made meaning NatWest isn't liable to reimburse him under the CRM Code. NatWest followed Mr R's instructions to make the payments, and for reasons explained, I'm persuaded he would have proceeded with these payments and wouldn't have heeded any warnings or risks that NatWest might have put forward. Unfortunately, given the funds Mr R transferred were exchanged into cryptocurrency and moved on, no funds remained that could be recovered.

My final decision

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 1 March 2024.

Matthew Horner
Ombudsman