DRN-4708566

The complaint

Mr W is unhappy National Westminster Bank Plc ("NatWest") won't reimburse him for the money he lost when he fell victim to a scam.

What happened

The details and facts of this case are well-known to both parties, so I don't need to repeat them at length here.
In short, Mr W says he saw an advert for a trading company on social media that I will call "B". Mr W completed an enquiry form and was contacted by a representative of B.

Subsequently, the following payments were made to two cryptocurrency exchanges. My understanding is that the funds were then converted to cryptocurrency and were transferred on to B.
The following transactions went from NatWest to the cryptocurrency exchanges.

Transaction Number	Date	Amount	Type of payment
1	13 June 2023	£5,000	Open Banking
2	14 June 2023	£9,000	Open Banking
3	14 June 2023	£9,000	Refund
4	14 June 2023	£932.47	Refund
5	14 June 2023	£10,000	Open Banking
6	3 July 2023	£20,520	Open Banking
7	6 July 2023	£30,000	Open Banking
8	20 July 2023	£29,000	Transfer
9	21 July 2023	£17,500	Transfer
10	28 July 2023	£12,500	Transfer
11	29 July 2023	£9,406.84	Transfer
12	29 July 2023	£10,000	Transfer
13	29 July 2023	£10,000.05	Transfer

(There were other payments made via transfers to a different third-party finance company. The payments to that company were dealt with separately at this service, so I will not comment on those payments).

Mr W realised that he had been scammed when he was told that he had to pay a large Anti Money Laundering fee in order to withdraw his profits.

He made a complaint via a representative to NatWest and requested that the above transactions be refunded. It declined to do this.

One of our investigators looked into this matter and he thought that NatWest should have intervened during transaction 2 and had it done so, it would have prevented the payments from being made. So they concluded that NatWest should therefore refund all of the above payments. He did though say that there should be a deduction of 50%, as he believed that Mr W was equally liable for his loss. NatWest did not agree and so this case has been passed to me to issue a 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.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

In broad terms, the starting position law is that NatWest is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in June 2023 that NatWest should:

- have been monitoring accounts and any payments made or received to counter various risks, including 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 firms are generally more familiar with than the average customer;

- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment; and

- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

It isn't in dispute that Mr W has fallen victim to a cruel scam here, nor that he authorised the payments he made by transfers to his cryptocurrency wallets (from where the cryptocurrency was subsequently transferred to the scammer).

So, I've gone onto consider, taking into account what NatWest knew about the payments, at what point, if any, it ought to have identified that Mr W might be at a heightened risk of fraud that merited an intervention.

Having considered the various factors, I think that NatWest needed to intervene during payment 2. I say this because this was a large payment and to a crypto exchange. Mr W was not in the habit of making large payments to crypto exchanges. I'm aware that cryptocurrency exchanges like B generally stipulate that transfers must go to an account held in the name of the account holder. NatWest would likely have been aware of this fact too. So, it could have reasonably assumed that the payments would be credited to a cryptocurrency wallet held in Mr W's name.

With this in mind, I've thought carefully about what a proportionate intervention, in light of the risks presented, would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to NatWest's duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

Taking that into account, I think NatWest ought, when Mr W attempted the first payment, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have intervened and asked Mr W about why he was making the payments. I note that Mr W later in the scam was not entirely forthcoming with the reasons that he was making the transactions in question. And later in the scam, he was lightly coached by the scammer on what to say. But early on in the scam, the relationship between the scammer and Mr W was not as close. Moreover, there is no indication of him being coached early in the scam. So had open and probing questions been asked early in the scam, I think that at the very least Mr W would have likely said that he was making the payments to invest in crypto. As NatWest detected remote access when they spoke to him later in the scam, I see no reason why it would not have detected this had it made an intervention earlier on. It think these two things combined would have given NatWest enough information to have issued a warning setting out the dangers of crypto investments.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. The warning NatWest ought fairly and reasonably to have provided should have highlighted in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for NatWest to minimise the risk of financial harm to Mr W. I think NatWest could've covered off the key features of scams affecting many customers, but not imposing a level of friction disproportionate to the risk the payment presented.

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case. And on the balance of probabilities, I think it would have. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mr W's payments. For example, Mr W finding the investment through social media, being assisted by a broker and being asked to download remote access software so they could help him open cryptocurrency wallet.

So, I think NatWest would have been concerned by what the conversation would most likely have revealed and so warned Mr W. Had it done so, I think Mr W would have listened and recognised he was at risk of being a victim of a scam especially given the FCA warning about B at the time.

It therefore follows that I think Mr W would not have gone ahead with the payments had NatWest provided Mr W with a warning during an intervention.

I've considered carefully whether Mr W should hold some responsibility for his loss, by way of contributory negligence. In this instance, the conversations between Mr W and the scammer were informal and unprofessional given the sums involved. I am also mindful that there was an FCA warning prior to Mr W sending funds to B. Again, given the amounts involved in this scam, I really think that Mr W should have at least done an online search on B, prior to sending the amount of funds that he did. Finally, I think that the scam could have been stopped early had Mr B been more forthcoming when NatWest did intervene later in the scam.

So overall and having considered everything, I think that Mr W contributed to his own loss and therefore I feel that it would be appropriate to reduce the amount of compensation due to Mr W by 50%.

I have thought about whether NatWest could have recovered the funds but the Contingent Reimbursement Model ("CRM") does not apply to funds sent to an account in the consumers own name. I also don't think that there was any other way to recover the funds.

Putting things right

So to put things right, I require NatWest to do the following:

- Refund 50% of the transactions Mr W lost to the scam, from and including payment 2, minus any credits received after this point; and

- Add 8% simple interest annually on those sums, calculated from the date they were paid to the date of settlement, less any tax lawfully deductible.

My final decision

Because of the reasons given above, I uphold this complaint in part and require National Westminster Bank Plc to pay the redress outlined above to put matters right, in full and final settlement of this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 10 January 2025.

Charlie Newton
Ombudsman