DRN-4325550

The complaint

Mr B is unhappy that National Westminster Bank Plc ("NatWest") will not refund the money he lost as the result of a scam.

Mr B has used a representative to bring his complaint to this service. For ease, I will refer solely to Mr B throughout this decision.

What happened

Both parties are familiar with the details of the scam, so I will provide only a summary here.

Mr B came across a company that I will call C. This company purported to be a crypto trading firm. C told Mr B that if he invested with it, he would receive profits every two weeks.

Between 16 September 2022 and 27 November 2022 Mr B made over 75 transactions, totalling over £130,000 to various crypto exchanges, from which the funds were sent firstly to C. When Mr B was unable to withdraw funds from C, he started sending funds to a company that promised to recover the funds on his behalf. When the second company did not recover Mr B's funds, he then realised he had been scammed twice.

I issued a provisional decision on 18 January 2024 in which I said the following;

"I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

There's no dispute that Mr B made and authorised the payments. Mr B knew who he was paying, and the reason why. At the stage he was making these payments, he believed he was transferring funds to invest in cryptocurrency. I don't dispute Mr B was scammed and he wasn't making payments for the reason he thought he was, but I remain satisfied the transactions were authorised under the Payment Services Regulations 2017.

It's also accepted that NatWest has an obligation to follow Mr B's instructions. So, in the first instance Mr B is presumed liable for his loss. But there are other factors that must be considered.

To reach my decision I have taken into account the law, regulator's rules and guidance, relevant codes of practice and what was good industry practice at the time. To note, as the payments were to an account in Mr B's name the principles of the Contingent Reimbursement Model (CRM) code do not apply in this case.

Nevertheless, I still think that NatWest should have:

been monitoring accounts and payments made or received to counter various risks, including fraud and scams, money laundering, and the financing of terrorism.

had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (amongst other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which financial institutions are generally more familiar with than the average customer.

in some circumstances, irrespective of the payment channel used, taken additional steps or made additional checks before processing a payment, or in some cases declined to make a payment altogether, to help protect its customers from the possibility of financial harm.

In this instance, I think that NatWest should have intervened earlier in the scam. Specifically on the third payment on 20 September 2022. This was the third payment in the day totalling over £10,000 to a relatively new payee that was, by my understanding, a crypto exchange. This was after 5 transactions had taken place to the same payee over the previous few days. Multiple transactions to a new account in the same day was unusual for Mr B's account.

I think that NatWest should have been aware that multiple payments in quick succession to a new payee especially a crypto exchange should really have alerted NatWest that something unusual was going on.

NatWest is aware of the typical patterns of scams like this – that customers often move money onto a crypto exchange account in their own name, before moving it on again to scammers. I also think that NatWest is aware that scams like this commonly take place with multiple payments, typically within quick succession of each other. So I think that there were enough indicators that NatWest should really have intervened around when the third payment was made on 20 September 2022, and that it should've asked questions about what the payments were for. And as they were being sent to a crypto exchange, I don't think it was unreasonable to expect NatWest to have asked questions about the nature of the 'investment'.

I appreciate that Mr B's loss didn't materialise directly from his NatWest account in these circumstances. But even though he was transferring funds to a crypto exchange account in his own name, I still think that NatWest ought to have taken a closer look at payment 2 – given the significant risk of fraud associated with cryptocurrency investments at the time.

The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018. And by January 2019, cryptocurrency scams continued to increase in frequency. So, by the time Mr B started making his 'investments' in 2022, it is reasonable to say NatWest ought to have had a good enough understanding of how crypto scams works – including the fact that their customers often move money to an account in their own name, before moving it on again to the fraudster.

Therefore, I'm satisfied that NatWest should've had mechanisms in place to detect and prevent this type of fraud at the time Mr B was making this payment, and that it should have led to it intervening to ask further questions about the payment in question.

I note that Mr B had made larger transactions in the months prior to the scam. But I am mindful that the prior large transactions differed to one to a new crypto exchange account. I say this as they were sent to HMRC and someone's bank account - so I don't think that this means that making a series of large transactions to a new crypto exchange account on the same day would seem like normal activity. So taken together, they are sufficiently different than the payment highlighted by NatWest that by the time of the third transaction on 20 September 2022, I think that it should have been clear that this was unusual for Mr B an had the hallmarks of a scam.

In terms of what the intervention should've looked like, I would expect NatWest to have intervened and asked Mr B who the payment was for; what it was for; and for the context surrounding the payment. It could, for example, have asked how he had been contacted; whether he'd parted with personal details in order to open a trading account; whether he was being helped by any third parties e.g. a broker; and how he had come across the investment, in this case via an unsolicited WhatsApp message.

I have no reason to believe Mr B wouldn't have been open with NatWest, had it intervened. And I think he would have taken its intervention seriously. So, I think NatWest would have quickly learned from a conversation with Mr B the basic background to the payment instruction – that he was intending to buy cryptocurrency which was sent onto what he thought was a cryptocurrency type trading investment and that a broker would 'trade on his behalf'.

Even though the conversation would have identified the payment was going to Mr B's own account (before being sent onto the scammers), the conversation shouldn't have stopped there on the basis that the money appeared to be going to somewhere safe and within Mr B's control. This is because, by 2022, NatWest was well aware – or ought to have been well aware – of how scams like this work – including that the customer often moves money onto an account in their own name before moving it on again to scammers.

So, I think NatWest would have been concerned by what the conversation would most likely have revealed and so warned Mr B, explaining the typical characteristics of scams like this.

Had it done so, I think Mr B would have listened and recognised he was at risk. I am satisfied he would have had second thoughts if NatWest had intervened effectively given that a warning would be coming from his trusted bank.

It follows I think Mr B would not have gone ahead with payment three on 20 September 2022, nor any subsequent payments.

I've considered carefully whether Mr B should hold some responsibility for his loss by way of contributory negligence.

In this instance, Mr B has explained that he had not done any research on C. From the correspondence between him and the scammer, it is clear that he was promised unrealistic returns - such as increasing his investment from £3,000 to £75,000 in two weeks. Mr B has explained that he had some investment experience, albeit not in crypto investing, but even though his experience did not include crypto, I think it would've been clear to anyone with even basic investing experience that the returns promised of over 2000% in two weeks is more than a little unrealistic and should have caused him some concern as to whether what he was being promised was real.

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

I note NatWest's comments that it believes that the crypto exchange that Mr B sent his funds to are also under this service's jurisdiction and therefore a complaint should be raised with them. But I am required to consider the case in front of me and I do not think that it would be fair to reduce the award that I am proposing because of this - as NatWest could have prevented Mr B's loss if it had intervened appropriately.

Putting things right

So currently, I intend to tell NatWest to:

- *Refund 50% of the disputed transactions plus associated fees from and including payment three on 20 September 2022 (the payment of £4,525.17 as it appears on Mr B's statement).*

- *Pay 8% simple interest, per year, on these transactions from the date of each transaction to the date of settlement, less any deductible tax."*

Mr B agreed with my provisional decision. NatWest did not and raised a number of points including the following;

- NatWest are not accountable or liable for this loss considering all the relevant regulation.

- What regulations and best practice am I referring to that led to my decision as they are concerned that I am essentially introducing additional regulation which are not supported by legislation and offers protection in addition to the carded scheme rules.

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.

Firstly, I should highlight that we have set out our position in a number of decisions and conversations with NatWest in relation to our approach on cases like this one. So I am not going to go into a great deal of depth in relation to all the points raised.

In relation to the regulation and best practice I was referring to in my provisional decision and why I believe that NatWest is accountable and liable for Mr B's loss, NatWest ought fairly and reasonable to have done the following;

- FCA regulated banks are required to conduct their "business with due skill, care and diligence" (FCA Principle for Businesses 2) and to "pay due regard to the interests of its customers" (Principle 6)[1].

- Banks have a longstanding regulatory duty "to take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime" (SYSC 3.2.6R of the Financial Conduct Authority Handbook, which has applied since 2001).

- Over the years, the FSA, and its successor the FCA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by banks to counter financial crime, including various iterations of the "Financial crime: a guide for firms".[2]

- [1]Regulated banks are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship).

- The October 2017, BSI Code, which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code, but in my view the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now.

- NatWest is also a signatory of the CRM Code. This sets out both standards for firms and also situations where signatory firms will reimburse consumers. The CRM Code does not cover debit card payments, but I consider the standards for firms around the identification of transactions presenting additional scam risks and the provision of effective warnings to consumers when that is the case, represent a fair articulation of what I consider to be good industry practice generally for payment service providers processing transactions.

In reaching my decision about what is fair and reasonable, I have taken into account that Mr B paid money to an account in his own name, rather than directly to the fraudster. So he remained in control of his money after he made the payments from his NatWest account, and the money took further steps before the money was lost to the fraudsters.

But for the reasons I have set out above, I am satisfied that it would be fair to hold NatWest responsible for Mr B's losses (subject to a deduction for his own contribution). As I have explained, the potential for multi-stage scams ought to have been well known to NatWest by the time that Mr B was the victim of a scam. And, as a matter of good practice, it should fairly and reasonably have been on the look-out for payments presenting an additional scam risk, including those involving multi-stage scams.

---

[1]Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

[2]For example, both the FSA's Financial Crime Guide at 4.2.5G and the FCA's 2015 "Financial crime: a guide for firms" gave examples of good practice in relation to investment fraud saying:
"A bank regularly assesses the risk to itself and its customers of losses from fraud, including investment fraud, in accordance with their established risk management framework. The risk assessment does not only cover situations where the bank could cover losses, but also where customers could lose and not be reimbursed by the bank. Resource allocation and mitigation measures are informed by this assessment.
A bank contacts customers if it suspects a payment is being made to an investment fraudster. A bank has transaction monitoring rules designed to detect specific types of investment fraud. Investment fraud subject matter experts help set these rules."

I'm satisfied NatWest should fairly and reasonably have made further enquiries before the third payment on September 2002 was made and, if it had, it is more likely than not that the scam would have been exposed. Had that happened, I don't think that Mr B would have lost any more money. In those circumstances, I am satisfied it is fair to hold NatWest responsible for Mr B's loss.

Finally, I have considered whether NatWest could have recovered funds via other means. My understanding is that all of the payments were made via debit card. So due to this and due to the payments being sent to an account in his own name, the CRM does not apply. Also a chargeback would not have been successful as Mr B essentially got what he had paid for - which was crypto currency, before forwarding it onto the scammer. So I don't think that funds could have been recovered via other means.

Putting things right

So I uphold this complaint in part and require NatWest to do the following:

- Refund 50% of the disputed transactions, plus associated fees, from and including payment three on 20 September 2022 (the payment of £4,525.17 as it appears on Mr B's statement).

- Pay 8% simple interest, per year, on these transactions from the date of each transaction to the date of settlement, less any deductible tax.

My final decision

Because of the reasons above, I uphold this complaint and I require National Westminster Bank Plc to pay the redress outlined above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 15 March 2024.

Charlie Newton
Ombudsman