

Complaint

Mr W is unhappy that National Westminster Bank Plc (NatWest) hasn't reimbursed him after he fell victim to a scam.

Background

The background to this complaint is well known to the parties and was set out in considerable detail in the Investigator's view. I don't intend to repeat it in full here, but I'll summarise it.

In 2022, Mr W fell victim to a scam. He'd purchased a bond several years earlier from a company that later entered administration. In September 2022, he was contacted by someone who said they were a representative of another company (that I'll refer to as S). They told him that the company Mr W had invested with had appointed S and they could help him get his money back. Mr W looked up S on Companies House and saw that it was a genuine limited company, although it now appears that company wasn't involved and the fraudsters simply imitated a genuine company. The communications Mr W received from the scammers were generally professional in tone and appeared credible and so he was persuaded that he was dealing with a legitimate operation.

Mr W was asked to make several payments in connection with this apparent attempt to recover his investment. He was initially told that he'd need to pay an early termination fee – he made two bank transfers to a named individual. The scammers said that person was a solicitor working for S. In October 2022, he was told that a sum of a little over £22,000 had been set aside to be refunded to him. However, he was told that he'd need to pay £6,300 to a *“capital exchange programme”* but, as far as I can see, no further details were provided on what this process was or why it was necessary. At the time, I understand Mr W had problems with his online banking facility. The scammer recommended that he send cash by recorded delivery, which Mr W agreed to do.

He was then invoiced again for a further payment of over £10,000. He was told this was for the *“payment gateway”* but I can't see that any explanation was offered for this by the scammers. He was asked to make a payment to a different person's account – he was told that this was a different solicitor who was working for S. He was then told that payments had been made outside of the necessary timescales and so penalties would be applied. Mr W would need to pay these to get his investment back.

It was only in November 2022 when the scammers sent Mr W another invoice (this time for £9,000) that Mr W spoke to a family member and ultimately recognised that it had been a scam throughout.

In total, Mr W transferred £21,176 in connection with the scam. Those payments were sent or withdrawn from two accounts he has with NatWest – one of these is an international account he holds with a subsidiary of NatWest in the Channel Islands, the other is a NatWest account he holds in the UK. He complained to NatWest via a professional representative, but it didn't agree to refund his losses. It assumed that, because Mr W had made payments to what he believed was a genuine limited company, this was primarily a

civil dispute which should be resolved through the courts.

Mr W was unhappy with that and so he referred his complaint to this service. It was looked at by an Investigator who didn't uphold it. He wasn't persuaded that NatWest ought to have recognised that there was a risk Mr W was falling victim to a fraud, and so it didn't do anything wrong by not intervening.

Mr W disagreed with the Investigator's view and so the complaint has been passed to me to consider and come to a final decision.

Findings

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

As I explained above, Mr W made payments from two accounts – one was a UK account and the other an international account. Most of his losses occurred on the international account. Unfortunately, this service doesn't have the power to consider any complaint about those payments or any alleged failings by NatWest in connection with them.

The rules that set out this service's powers say that we can consider complaints about the activities of firms which are carried on from an establishment in the United Kingdom or a European Economic Area (EEA) state. Those rules define '*United Kingdom*' as "*England and Wales, Scotland and Northern Ireland (but not the Channel Islands or the Isle of Man)*" Most of the payments made in connection with the scam were made from an account operated by a firm operating out of the Channel Islands and so I don't have the power to consider them.

There are two transactions that I am able to look at. They are a £5,000 counter withdrawal which Mr W made when he'd agreed to send cash to the scammers by post and, later, a £2,650 bank transfer made by Faster Payments to a personal account that the scammers said was their solicitor. I've dealt with each separately.

The cash withdrawal

The starting position would be that NatWest was obliged to honour Mr W's request to make a withdrawal from his account. However, good industry practice required that it be on the lookout for account activity that was unusual or out of character to the extent that it might indicate its customer was at increased risk of financial harm due to fraud. On spotting such a risk, I'd expect it to intervene in a manner proportionate to the risk it had identified.

With the benefit of hindsight, it is now known that Mr W had been targeted by a fraudster and he was withdrawing the cash on their instructions. However, the question I have to consider is whether NatWest ought to have recognised that risk and intervened to protect Mr W from it.

Unfortunately, I'm not persuaded it would've had any reasonable basis for treating this withdrawal as unusual or out of character. I've looked at the statements for Mr W's account in the months leading up to the scam. It's not an account with a large volume of transactions, but there were still payments that were significantly larger than this one.

I also understand that Mr W was asked what the withdrawal was for, and he told an employee of the bank he was withdrawing the cash to help his son. Even if an employee of the bank had questioned the payment with him, it seems very unlikely that they'd have been able to get to the bottom of what was really going on here and so I don't think it did anything wrong in allowing him to make the withdrawal.

The bank transfer

This payment falls within the scope of the Lending Standards Board's Contingent Reimbursement Model (CRM) Code. The starting point under the Code is that firms should reimburse customers who fall victim to authorised push payment (APP) scams like this one. However, NatWest doesn't need to reimburse Mr W if it can show that one of the Code's exceptions applies. The most relevant exception is where *"the customer made the payment without a reasonable basis for believing that ... the person or business with whom they transacted was legitimate."*

I've considered this point carefully and, while I recognise that Mr W made this payment with the sincere belief that they were connected to a legitimate purpose, I'm afraid I'm not persuaded that belief was a reasonable one. I'm surprised that he wasn't more concerned at the request that he make payments to personal accounts. I recognise he was told that those individuals were solicitors working on behalf of the company he was dealing with. But a legitimate solicitor wouldn't ask for client money to be paid into a personal account and I think Mr W ought to have found the proposal concerning, particularly given his professional background as a former chartered accountant.

He was also asked and agreed to make several large payments as part of the process of getting his investment back but doesn't appear to have been given any explanation as to what these payments were for or why they were necessary. Finally, I think Mr W should've been concerned when it was suggested that he pay one of the fees by sending cash in the post. I think he ought to have recognised that this would be an unorthodox way for a legitimate business to operate. It's also significant that, although the company that the scammers were imitating had a trading address in a commercial premises in a market town in the south of England, he was asked to send the cash to a residential address in a completely different area of the country.

I'm also satisfied that NatWest met its standards under the Code. It ought to provide its customer with effective warnings where an APP scam risk is identified, for example if there is payment activity that is unusual or out of character. But given that Mr W had made larger payments from his account in the months prior to the scam, I don't think it would've had any reasonable basis for doing so here.

I've also considered whether NatWest did everything it should once it was notified of the scam. In respect of the cash withdrawal, there wasn't anything it could do to help Mr W recover the money. With the transfer, I'd expect NatWest to make contact with the bank that operated the receiving account to see whether any of the funds remained in the account. However, Mr W made this payment on 24 October 2022. The bank wasn't notified about the scam until February 2023. Fraudsters will typically move on funds as quickly as possible. So by the time NatWest was told what had happened, there was no realistic prospect of recovering any of Mr W's money from the receiving account.

Final decision

For the reasons I've set out above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 19 April 2024.

James Kimmitt
Ombudsman