DRN-5173160

Complaint

Ms J is unhappy that National Westminster Bank Public Limited Company ("NatWest") didn't reimburse her after she reported falling victim to a scam.

Background

In 2022, Ms J began communicating with a man she met on an online dating website. After exchanging messages, an apparent relationship developed between the two. Unfortunately, Ms J didn't realise it at the time, but the man who had contacted her wasn't genuine. She'd been targeted by a fraudster.

I understand they spoke on the phone, but never met in person. He told her that he worked in the United States Navy and, as a result, was often travelling for work. That meant that meeting in person wasn't straightforward. Ms J says that she looked up the name of this man on various social media platforms. She found profiles that were consistent with the person who'd contacted her and so this persuaded her that she was dealing with a genuine person.

After a short while, he started to ask Ms J for financial support. He asked that she make payments to help him with various expenses and asked that he make them to accounts in the names of other individuals. One account that she paid, for example, was supposedly an account in the name of her contact's boss. She made multiple payments over a period between June 2022 and May 2023. Her total losses were a little under £9,000.

Once she realised that she'd fallen victim to a scam, she notified NatWest. It didn't agree to refund her. It said it had provided her with warning messages when she was making the payments online. It also didn't think that it did anything wrong in failing to conduct fraud checks in connection with any of the payments.

Ms J wasn't happy with that response and so she referred her complaint to this service. It was looked at by an Investigator who didn't uphold it. Ms J disagreed with the Investigator's opinion 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.

The starting point under the relevant regulations (Payment Services Regulations 2017) is that customers are liable for transactions that they have authorised. There's no dispute here that all these transactions were authorised by Ms J and so she is presumed liable at first instance. However, that isn't the end of the story. Some of these payments were covered by something known as the Contingent Reimbursement Model Code (CRM Code). Firms that signed up to the CRM Code are expected to reimburse customers who fall victim to authorised push payment (APP) scams like this one in most circumstances. There are, however, exceptions in the rules. If one of those exceptions applies, the firm isn't expected to pay a refund.

There are other obligations too that apply to all the payments, including those ones not covered by the CRM Code. Briefly summarised, good industry practice required that NatWest be on the lookout for account activity or behaviour that was unusual or out of character to the extent that it might have indicated Ms J might be at risk of financial harm due to fraud.

I've considered each set of requirements separately in the findings that follow.

CRM Code

All the payments that were made by bank transfer in connection with this scam are covered by the CRM Code. As explained above, a firm can choose not to reimburse a customer where it can show that one of the exceptions applies. The most applicable here is R2(1)(c) which applies where *"the Customer made the payment without a reasonable basis for believing that … the person or business with whom they transacted was legitimate."*

I appreciate that Ms J did sincerely believe that she was making these payments to a genuine individual and that there was a relationship between them. Unfortunately, I'm not persuaded that belief was a reasonable one. I can't ignore the fact that she made the payments to someone who she'd never met in person and who appears to have begun to ask her for financial support fairly early on.

As far as I can see, the reasons given as to why he needed financial support weren't particularly compelling either. For example, it's not clear why someone who was working for the US Navy and on tour would need someone to provide him with financial support to cover transport costs. I also think she ought to have been concerned at being asked to make payments to the personal accounts of individuals other than the man she'd been exchanging messages with. There doesn't appear to have been a good reason why he couldn't receive funds himself. I also think she should've been more sceptical about being asked to pay, for example, the fraudster's boss. Both individuals were apparently enlisted in the US Navy but made use of UK bank accounts.

I don't know how the fraudster explained these things to her and overcame any scepticism she might have had because she's only been able to provide a partial history of communications between her and the fraudster from the end where the scam unravels. I accept that she was manipulated by the fraudster into thinking that his requests were reasonable. Nonetheless, I think she should've proceeded with more caution here than she did and so I don't find that she made these payments with a reasonable basis to believe that she was paying a legitimate person.

The CRM Code also provides that, where a customer is *"vulnerable"* according to its own definition, the exceptions to reimbursement should be disapplied. Its definition says that a customer is vulnerable if *"it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered."*

I've also considered whether this definition would apply to Ms J and I'm not persuaded that it does. I can see that she has clearly suffered with poor mental and physical health in recent years. Her representatives have pointed out that she suffered a pulmonary embolism in February 2023. But this comes after all but one of the payments covered by the CRM. I can also see that she has suffered with significant depression and has been prescribed sertraline. However, that course of treatment didn't begin until after the scam had taken place so it's difficult to make a compelling argument that her depression meant she wasn't able to protect herself from the scam at the time it occurred. Overall, I'm not persuaded that the CRM Code's definition of vulnerability applies to her in this set of circumstances.

Other considerations

As I explained above, the firm is expected to be on the lookout for out of character payments. If it suspects a customer is at risk of financial harm due to fraud, it should take steps to protect the customer from that risk. That might be as simple as displaying a warning as part of the payment process, but it might extend to pausing a payment and contacting the customer to establish the wider circumstances before deciding whether it should be processed. Any steps a firm takes in response ought to be proportionate to the risk presented by the payment.

We now know with the benefit of hindsight that Ms J was falling victim to a scam. The question I have to consider is whether that risk ought to have been apparent to NatWest at the time. I've considered that carefully and I'm not persuaded that it ought to have recognised the risk here. The individual payments were generally of low value (even though I accept that, in total, it resulted in a significant loss). They were also made to several different payees – so that would've made it harder for NatWest to recognise that they were all being made in connection with the same scam. I understand that, in connection with two of the payments, there was a light touch intervention – NatWest contacted Ms J to check that she had indeed authorised the payments in question, but no detailed conversation took place. Overall, I don't think it would be reasonable to have expected NatWest to have spotted the risk of fraud here and so I'm not persuaded that it did anything wrong where it processed them without intervention or where it intervened in a non-interventionist way.

For the sake of completeness, I've also looked into whether NatWest did everything it should've done to recover Ms J's money after the event. It's expected to take reasonable steps to request the return of funds from the receiving bank – i.e. the bank that operates the account used by the fraudster. However, this scam played out over an extended period of time and, as a result, there had been a significant delay between the payments being made and it being reported to NatWest. From the cases we see, fraudsters tend to move on fraudulently acquired funds as quickly as possible and so I'm afraid the prospect of recovering any funds from the receiving accounts was already remote.

In respect of card payments, a bank can raise a chargeback on behalf of its customer. However, as the Investigator explained in her view of the complaint, that needed to be done within 120 days for it to be valid and that wasn't the case here.

I don't say any of this to downplay the fact that Ms J has fallen victim to a cruel and cynical scam. I have a great deal of sympathy for her and the position she's found herself in. However, my role is to look at the actions and inactions of the bank and I'm satisfied it hasn't done anything wrong here.

Final decision

For the reasons I've explained, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms J to accept or reject my decision before 11 July 2025.

James Kimmitt
Ombudsman