DRN-5977812

The complaint

Miss S complains that NATIONAL WESTMINSTER BANK PUBLIC LIMITED COMPANY ('NatWest') hasn't refunded the money she says she lost to an authorised push payment ('APP') scam.

What happened

The circumstances of the complaint are well-known to both parties. So, I don't intend to set these out in detail here. However, I'll provide a brief summary of what's happened.

Around October 2022, Miss S met a third party (whom I'll refer to as 'A') online. Miss S believed that she and A had entered into a romantic relationship. A said they had experience investing in cryptocurrency and persuaded Miss S to make an investment. A told Miss S to send funds to an unknown third party, after which she was able to track her investment through two genuine cryptocurrency tracker apps.

Miss S says that the investment appeared to grow and so she asked to make a withdrawal. Between November 2022 and November 2023, Miss S made faster payments to A and other unknown third parties. Miss S also says that A opened accounts with several online casinos, and she authorised payments to those accounts which A had made using her debit card details.

Miss S did receive some funds from A; the other beneficiaries she paid; and from the online casinos. However, she has suffered a loss of approximately £50,000. Believing A had scammed her, Miss S asked NatWest to reimburse her.

NatWest said that it wasn't responsible for reimbursing Miss S's loss, as it considered the situation to be a private matter between Miss S and A, as Miss S and A had been involved in a romantic relationship. NatWest did recognise that its customer service could've been better when Miss S reported the situation to it and NatWest apologised for the impact this had on her.

Unhappy with NatWest's response, Miss S referred her complaint to this service. Our Investigator considered the complaint but didn't uphold it. In summary, they said there wasn't enough evidence to say Miss S had been the victim of an APP scam, meaning NatWest wasn't responsible for refunding her loss.

Miss S didn't accept our Investigator's opinion. She argued that she'd provided enough evidence to suggest an APP scam had taken place and that NatWest should reimburse her loss. As an agreement couldn't be reached, the complaint was passed to me to decide.

After reviewing the complaint, I was satisfied Miss S had, most likely, been the victim of an APP scam. However, I wasn't persuaded NatWest was responsible for refunding Miss S's loss. As I'd reached a different outcome to our Investigator, I issued a provisional decision setting out the reasons why I didn't think NatWest needed to reimburse Miss S.

NatWest didn't respond to my provisional decision, but Miss S said she didn't agree. She said she'd been able to track her investment using genuine cryptocurrency tracker apps, which showed her balance increasing, which made the scam believable.

Miss S also thought NatWest ought to have recognised she was at risk of financial harm when the scam payments were made and done more to protect her. Had that happened, Miss S was of the opinion that it would've prevented the scam payments being made.

As an informal agreement hasn't been reached, I'm now proceeding to issue my final 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.

Having done so, and after reviewing Miss S's response to my provisional decision, I see no reason to depart from my provisional findings, which I'll reiterate below.

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

Having done so, I've reached the same outcome as our Investigator, but for different reasons. I'll explain why I don't think NatWest needs to do anything further to resolve Miss S's complaint.

Miss S has explained that most of the correspondence relating to the disputed payments is no longer available. But she has provided some evidence of the communication between her, A, and some other third parties. Whilst these messages don't set out what each individual disputed payment was for, they do give an overall understanding about what's happened.

Having reviewed the messages, I think they are consistent with a romance/investment scam which Miss S has alleged has happened here. And I think it's likely that Miss S has sent payments for the purpose she's explained – i.e., she sent money to various payees to invest in a cryptocurrency investment and to facilitate the withdrawal of her funds. So, unlike our Investigator, I'm satisfied that Miss S has more likely than not been the victim of an APP scam. So, I've considered whether NatWest ought to reimburse Miss S's loss.

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.

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

It's not in dispute that Miss S made the scam payments. So, the payments were authorised and under the Payment Services Regulations, the starting position here is that Miss S is responsible for the payments (and the subsequent loss) despite the payments being made as the result of a scam.

However, that isn't the end of the story. At the time Miss S made the scam payments, NatWest was signed up to the Lending Standards Board's Contingent Reimbursement Model ('CRM') Code, which was in place until 6 October 2024. The CRM Code provided additional protection to consumers who had been the victims of APP scams like this, in all but a limited number of circumstances.

The payments Miss S authorised to the online casinos aren't caught by the principles of the CRM Code. That's because the CRM Code doesn't cover debit card payments. So, whilst the payments were made because of a scam, Miss S's payments to the online casinos don't meet the required criteria for the CRM Code to apply.

However, the faster payments Miss S made to A and approximately 15 other beneficiaries are caught by the CRM Code and so I've considered whether Miss S reasonably ought to have been reimbursed by NatWest.

Not all scam payments covered by the principles of the CRM Code are required to be reimbursed. Under the CRM Code there are exceptions to reimbursement. Relevant to this complaint is R2(1) of the CRM Code, which states:

> *"A Firm may choose not to reimburse a Customer if it can establish any of the following matters in (a) to (e). The assessment of whether these matters can be established should involve consideration of whether they would have had a material effect on preventing the APP scam that took place…*
>
> *(c) In all the circumstances at the time of the payment, in particular the characteristics of the Customer and the complexity and sophistication of the APP scam, the Customer made the payment without a reasonable basis for believing that:*
>
> *(i) the payee was the person the Customer was expecting to pay;*
> *(ii) the payment was for genuine goods or services; and/or*
> *(iii) the person or business with whom they transacted with was legitimate…"*

I've carefully considered Miss S's testimony and the evidence she's provided of the scam. I'm really sorry to disappoint Miss S, but I think a valid exception to reimbursement applies in this case, specifically that Miss S made the scam payments without a reasonable basis for believing that the persons with whom she transacted with were legitimate. I'll explain why below.

Miss S made the scam payments based on information she received from A and other third parties via social media. When she began making the payments, she hadn't met any of the individuals she sent money to or those that had told her to make payments. I've seen nothing to suggest Miss S attempted to verify who these individuals were or what their experience was in investing in cryptocurrency.

Miss S hasn't been able to explain how her investment with A was supposed to work. So, I can't say the premise of the investment was plausible. Also, A told Miss S that if she invested, she would make a return of 500%. That rate of return is clearly too good to be true and ought to have given her cause for concern. As should the fact that she hadn't signed a contract with A setting out the terms and conditions of her investment. So, even to an inexperienced investor like Miss S, there were warning signs that something wasn't right.

From the messages I have seen, I'm not persuaded Miss S was ever given a plausible explanation for why she needed to pay funds to withdraw from her investment. And, she continued to make payments, despite A failing to keep to his promises of returning Miss S's funds. I've seen very little evidence to demonstrate that Miss S had a reasonable basis for believing A was legitimate and so I don't think she had a reasonable basis for believing she was making payments for a genuine reason.

Whilst I've established that Miss S didn't have a reasonable basis for belief, I also need to consider whether NatWest met its expectations under the CRM Code, which required it to give an effective warning when it identified (or reasonably ought to have identified) an APP scam risk.

The scam payments covered by the principles of the CRM Code were spaced out over a period of 12 months. Generally speaking, the payments weren't so large that the value alone ought to have given NatWest cause for concern. Whilst there was a large number of payments, often these were low value and spaced out, preventing the scam being identified and didn't create a pattern of activity that was indicative of fraud. So, I don't think the pattern of the payments indicated a scam risk to NatWest at the time the payments were made. As a result, I don't think NatWest needed to provide Miss S with an effective warning, with the exception of one payment.

There was a scam payment, for £5,000, which did stand out as being unusual as it was larger than Miss S's typical payments activity and the payment was made a day after Miss S had sent the same payee £2,500 (taking the total sent to that individual to £7,500 in a short period of time). So, NatWest ought to have identified that the £5,000 payment demonstrated an APP scam risk and provided an effective warning when that payment was made. NatWest hasn't been able to show what warning it gave. As a result, I can't say it met its expectations (under the CRM Code) when that payment was made.

However, to say that Miss S ought to receive a refund for that payment, I'd need to be satisfied that an effective written warning would've had a material effect on preventing the payment being made. And, in these circumstances, I'm not persuaded it would've done.

At the time of the payment, Miss S had been making payments towards the scam for around six months. So, it seems Miss S believed that she was making payments for a genuine reason and believed doing so would've resulted in A being able to return her funds. So, it seems unlikely that a written warning would've resonated with her at the time or stopped her proceeding with the payment. And any concerns that this might have caused Miss S would likely have been alleviated by A.

I'm also mindful that Miss S has alleged that throughout the scam A threatened her with violence, blackmailed her and coached her on how to send funds to avoid detection. So, even if NatWest had gone further than a written warning and spoken to Miss S about the payment, I'm not persuaded she would've given accurate answers about why the payment was being made. So, I'm not persuaded NatWest needs to reimburse Miss S because it failed to give an effective warning or intervened to question Miss S verbally, as this is unlikely to have had a material effect on preventing the loss.

I appreciate that falling victim to this scam will have been distressing for Miss S, especially as she's provided evidence that shows A was aggressive and threatening in some of his exchanges with her. She's also reported that he was blackmailing her into making some of the payments. Whilst I can understand how this might have impacted her decision making, I'm not satisfied this demonstrates that Miss S was vulnerable to this scam or that she couldn't have protected herself from the scam. And, as a result, I don't think she is entitled to reimbursement under the CRM Code.

I've thought about whether there are any other reasons, outside of the CRM Code, that would allow me to fairly hold NatWest responsible for Miss S's loss. Good industry practice required NatWest to be on the lookout for account activity or payments that were unusual or out of character to the extent that they might indicate a fraud risk. On spotting such a payment, I'd expect it to take steps to warn the customer about the risks of proceeding.

Based on the value and the pattern of the scam payments, I'm not persuaded NatWest reasonably ought to have been concerned that Miss S was at risk of financial harm from fraud to the extent that it ought to have intervened and questioned the payments. The value of the payments weren't so significant that the value alone made them appear suspicious. I accept there was a payment for £5,000 (which I've referred to above), which was larger than previous payments. However, I've already explained why I don't think NatWest would, most likely, have been able to prevent the payment being made if it had intervened and questioned why she was making the transaction.

I've seen no evidence to suggest NatWest contacted the beneficiary banks about Miss S's faster payments, which I'd have expected it to have done in the circumstances. However, the scam wasn't reported to NatWest until several months after the final payment had been made. So, it seems unlikely that any funds would've remained in the beneficiary accounts.

I've also thought about the debit card payments that were made to accounts with online casinos in Miss S's name. Although Miss S says the payments were made by A, she had to approve the payments. So, they are treated as authorised and Miss S is responsible for them in the first instance. Having reviewed the payments, I don't think a pattern of fraud was evident from the transactions, and so I don't think NatWest needed to intervene to question Miss S about the debit card payments.

As the merchants were genuine online casinos, it seems likely that any goods and services purchased would've been provided and that a chargeback would've likely been defended by the merchants. As a result, I don't think NatWest was wrong or unreasonable in not pursuing chargebacks that had little prospect of success.

Miss S has, most likely, been the victim of a cruel scam. Whilst I have natural sympathy with Miss S, I'm not persuaded NatWest could've prevented the loss or recovered the funds. I'm also not persuaded it should be held responsible for reimbursing Miss S's loss."

I appreciate that Miss S was given access to genuine cryptocurrency tracker apps, which allowed her to see the value of the cryptocurrency that had been purchased in her name. Whilst I can understand why this may have been persuasive to Miss S, I don't think it's enough to demonstrate that she had a reasonable basis for belief when she made the scam payments that are caught by the principles of the CRM Code.

There were multiple warning signs that this wasn't a legitimate investment opportunity and the manner in which the scammer conducted himself wasn't indicative of someone acting genuinely. However, despite the irregularities of what she was asked to do, Miss S simply followed the instructions of individuals she'd never met and sent funds to other third parties she didn't know either.

I think NatWest failed, on one occasion, to provide an effective warning under the CRM Code. However, as I explained in my provisional decision, I don't think an effective warning would've had a material effect on preventing the payment being made and I'm persuaded Miss S would, more likely than not, have gone ahead with the payment regardless. And I don't think NatWest needed to intervene when the other scam payments were made, including the debit card payments made to online casinos.

Miss S has explained how the scam has impacted her and I'm sorry that she's lost this money. Whilst I sympathise with her situation, I'm not satisfied NatWest can fairly be held responsible for the loss she's suffered. I don't think NatWest needs to reimburse any payments under the CRM Code, nor do I think NatWest reasonably could've prevented or recovered Miss S's loss. As a result, I'm not persuaded NatWest was incorrect when it declined to reimburse her.

My final decision

For the reasons explained above, and in my provisional decision, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 26 December 2025.

Liam Davies
Ombudsman