DRN-4871999

The complaint

X complains that National Westminster Bank Plc ("NatWest") did not refund a series of payments they say they lost to a scam.

What happened

X purchased three boats and was looking for a courier company to ship them overseas. After a few failed attempts, they found a company I'll call 'TF' for the purposes of this decision. TF quoted them £9,000 to send the shipment, and provided an invoice for the payment. Following this, X was told the vehicle that was due to pick up the trailer with the shipment had broken down and could not collect it. Following this there were a number of additional charges that TF said were necessary, due to increased fees by the shipping companies due to new routes being required. X made the following payments from their NatWest account to TF:

Date	Amount
22/08/2022	£5,000
23/08/2022	£4,000
18/10/2022	£310
27/10/2022	£160
05/11/2022	£350
08/11/2022	£350
28/11/2022	£400
13/01/2023	£565
22/05/2023	£500

In September 2023, when the shipment still had not been sent, X asked TF for a refund. TF confirmed a refund would be processed; however, X has not yet received this. X raised a scam claim with NatWest in November 2023 as they felt TF had taken their funds with no intention to ship the products. NatWest responded and said they felt this was more likely a civil dispute between X and TF, so they did not agree they needed to refund X in the circumstances.

X referred the complaint to our service and our Investigator looked into it. They explained that NatWest is signed up to the Contingent Reimbursement Model (CRM) Code which is a scheme that gives additional protection from Authorised Push Payment (APP) scams. However, in order to consider transactions under the code, they have to meet the definition of an APP scam. The investigator did not agree the definition of an APP scam had been met in this case, as TF was a limited company that had been incorporated since 2021, they had continued to correspond with TF five months after the final payment and the receiving bank information did not indicate X had been the victim of a scam.

X disagreed with the outcome and their representatives raised some additional points. They said:

- TF did not have an online presence and had many negative reviews.
- TF never evidenced the reason for delays or additional fees.

- The address TF listed did not belong to them.

As an informal agreement could not be reached the complaint has been passed to me for a 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.

It isn't in dispute that X authorised the payments in question. Because of this the starting position – in line with the Payment Services Regulations 2017 – is that they are liable for the transactions. But they say that they have been the victim of an APP scam.

NatWest has signed up to the voluntary CRM Code, which provides additional protection to scam victims. Under the CRM Code, the starting principle is that a firm should reimburse a customer who is the victim of an APP scam (except in limited circumstances). But the CRM Code only applies if the definition of an APP scam, as set out in it, is met. I have set this definition out below:

...a transfer of funds executed across Faster Payments…where:

(i) The Customer intended to transfer funds to another person, but was instead deceived into transferring the funds to a different person; or

(ii) The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent.

The CRM Code is also explicit that it doesn't apply to private civil disputes. The wording in the code is as follows:

"This Code does not apply to:

> *b) private civil disputes, such as where a Customer has paid a legitimate supplier for goods, services, or digital content but has not received them, they are defective in some way, or the Customer is otherwise dissatisfied with the supplier."*

I've therefore considered whether the payments X made to TF fall under the scope of an APP scam as set out above. Having done so, I don't agree that they do. I'll explain why in more detail.

In order to determine if X has been the victim of a scam, I have to consider if their intended purpose for the payments were legitimate, whether the intended purposes they and the company they paid were broadly aligned and, if not, whether this was the result of dishonest deception on the part of the company, in this case TF.

What was X's intended purpose for the payments?

From what I have seen, X's intended purpose of the payments was to facilitate the delivery of products they had purchased (in this case boats on a trailer). This was an international delivery via large ships, that would likely take some time to complete. Nothing I have seen indicates that X did not think this was a legitimate service that TF was providing.

What was TF's intended purpose for the payments?

X's representatives have alleged that TF did not intend to provide the service X had paid for and have pointed to a few things that they feel validate their arguments. For example, they have said TF did not have much of an online presence and had negative reviews.

However, I note that X said they found TF online, so there was enough of an online presence that they were able to find the company. And I've seen the negative reviews online, which do suggest there have been significant issues with other customers not receiving the service they paid for, but this alone does not indicate TF never intended to provide the service to X.

X's representative has also said that TF did not provide any evidence for the delays, but I cannot see that X asked them for evidence of this. Ultimately, it is for X to evidence that they have been the victim of a scam and provide the evidence they feel is relevant to show this.

I have reviewed the receiving bank statements for TF, that show what happened the X's funds once they were received into the account. For data protection reasons, I cannot share in detail what I have found. But I want to assure X that I have carefully reviewed this evidence to come to an outcome that I feel is fair. Having done so, I think there is enough activity related to X's purpose for the payments, around the same time that the payments occurred, for me to agree TF also intended to use the payments to facilitate the delivery of X's goods. I therefore think it is more likely that TF and X's intended purpose for the payments broadly aligned.

On balance, there are a number of points that I think raise concerns about TF as a company. The negative online reviews, the fact a refund still has not been provided to X and the address listed online is not correct according to X. But while these may show TF is not effective or professional as a company, I don't think they outweigh the evidence shown in the statements that support TF did intend to provide the service they were paid for. So, I don't think this meets the definition of an APP scam. With all of the above in mind, I think NatWest acted reasonably when it treated this case as a civil dispute.

It is possible that further evidence may come to light at a later date, which may indicate TF was operating a scam. Should such evidence come to light, then X can complain to NatWest again, and refer the matter to this office, should they not be happy with the outcome.

My final decision

I do not uphold X's complaint against National Westminster Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask X to accept or reject my decision before 20 February 2025.
Rebecca Norris
Ombudsman