DRN-4454274

The complaint

A company which I will refer to as 'C', complains that National Westminster Bank Plc won't reimburse the money the company lost following an Authorised Push Payment (APP) scam.

What happened

In May 2021, C made a payment of about £100,000 in the belief that they were paying one of their existing suppliers. Unfortunately, it turned out that C had fallen victim to a scam. By the time the scam was discovered and reported, only about £1,700 remained in the account where the money had gone.

C said that NatWest could have done more to prevent their loss. In particular, they say that when the payment was made, NatWest ought to have warned them that because it was a foreign payment there is no recourse under the Contingent Reimbursement Model Code ('the Code'), should something go wrong. C also said that the bank ought to have advised them not to send electronic payments abroad but to use cheques instead.

One of our investigators considered the complaint and concluded that it couldn't be upheld. In summary, they said that compared to the prior account activity, the relevant payment wasn't out of character or unusual. So, they can't say that the bank failed to intervene by way of providing a warning or otherwise when the payment was made. On being advised of the scam, NatWest immediately reported it to the recipient bank and therefore there was no failure in this regard as well. C says that NatWest failed to obtain the recipient's details, however the bank wouldn't be able to compel the recipient bank to disclose information about the recipient's account. Taking all of this into account, the investigator said that they couldn't recommend that the complaint be upheld.

C did not agree. Responding on behalf of C, their director reiterated that the bank ought to have warned C of the risks of making electronic payments abroad.

My provisional decision

I issued a provisional decision (which forms part of this decision), not upholding the complaint. I said:

> *"I thank C's director for providing detailed submissions to support the complaint, which I have read and considered in their entirety. I appreciate why he strongly feels that NatWest could have done more to help prevent C's loss. However, I trust that he will not take the fact that my findings focus on what I consider to be the central issues, and that they are expressed in considerably less detail, as a discourtesy. The purpose of my decision is not to address in detail every point raised but to set out my conclusions and reasons for reaching them.*
>
> *A lot has been said about the riskiness of making electronic payment abroad. However, the problem here occurred not so much because it was a payment abroad. The payment was correctly made to the account specified in the payment instruction. The problem*

principally arose because a fraudster intercepted an email exchange between C and its supplier and altered the bank details. Unfortunately, this was not deducted by C or their sub-contractor.

C has explained that when they get a request to change a bank account, their usual procedure is to contact the payee to verify the details. However, on this occasion that did not happen. C says that because the sub-contractor approved the invoice, it was assumed that they had in effect also authorised the change in the bank account. Therefore, the person making the payment did not carry out any further checks.

The payment instruction was then presented to the bank for payment. In broad terms, the starting position in law is that a bank is expected to process payments and withdrawals that its customer authorises it to make. However, there are circumstances where it might be appropriate for banks to take additional steps – as for example have systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud.

So, I reviewed C's account statements for a year or so prior to the payment to understand the general account activity and to determine whether on this occasion the bank ought to have intervened.

Over the period, I see that this was an active account with several large payments within the UK and abroad. The disputed payment was higher in value when compared to other payments made during this period. However, occasional higher payments could happen on an account. Further, whilst the amount was high, it represented a relatively smaller proportion of the balance on the account. It did not for example consume all or substantial proportion of the funds in C's account – which might have been an indicator it was at risk of fraud. The payment was to a new payee, but this alone wouldn't have given NatWest much cause for concern.

Given all this, I can't say that the payment stood out sufficiently from the prior account activity to reasonably have prompted NatWest to take further action. I'm not persuaded that there was enough here for me to find NatWest at fault for carrying out C's payment instruction in line with its primary obligation to do so.

C says a key issue here is the bank's failure to warn C that electronic payments abroad carry a higher risk. They are particularly unhappy that the bank did not warn them that because it was a payment abroad, there is no recourse under the Code should something go wrong.

The CRM Code is a voluntary code that covers certain type of transactions, and even in relation to those types of transactions whether there could be a successful claim under the Code depends on what happened in that specific case.

Further, not all the customers of a participating bank are eligible to make a claim under the Code. For example, a business customer wouldn't be able to make a claim if they are not a micro-enterprise. This is even for domestic payments.

There are specific rules and guidance to decide whether or not a business would fall under the definition of a micro-enterprise for this purpose. Broadly, a micro-enterprise, as defined in regulation 2(1) of the Payment Service Regulations is, an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million. In other words, an enterprise wouldn't be considered as a micro- enterprise for this purpose if it employs 10 persons or more; or if it employs less than 10 persons then if both its total gross assets and annual turnover exceed EUR 2

million. When determining whether these criteria are met, if the entity has any 'connected' enterprises, their figures will also need to be taken into account. In addition, the eligibility is determined based on the status at the time of the transaction.

From what I have seen, there is no requirement under the Code that where a particular transaction isn't covered under the Code, the bank should notify this to its customer when making the payment. Whilst it is always helpful if the bank could provide as much warning and information as possible to its customers, given all of the above, I can see why it could be difficult in practice to have such a requirement.

Nevertheless, in this instance, C was advised by their supplier (or so they thought) to pay to an account abroad. So even if C was made aware that the payment isn't covered by the Code, I consider it more likely they would have proceeded with the payment anyway because that is what their 'supplier' asked them to do.

I think the bank could have given generic warning about the scams of this nature. However, in this instance as previously noted, the payer believed that the sub-contractor had verified the payment details - to the extent that they didn't deem it necessary to call and check with the payee as they would have usually done. So, I think it is more likely than not that they would have proceeded with the payment in any case.

The director of C also strongly believes that the bank ought to have advised C that sending money abroad by way of cheque was safer. He believes that the banks should ban all electronic payments abroad and suggest to their customer that they should only use cheques. Firstly, a payment by cheque isn't also covered under the Code. Secondly, there are advantages and disadvantages in different modes of payments and a payment by cheque isn't devoid of risk. So, I am not persuaded that when C made this electronic payment NatWest automatically ought to have advised them to send the payment by cheque instead. Ultimately, I think it is for the company to decide how they would like to send the money abroad.

C's director also feels that because payments abroad aren't covered by the Code, the bank wasn't incentivised to 'chase' the fraudster. However, I can see that the bank promptly contacted the recipient bank abroad after being advised of the scam, put C's concerns to that bank and helped C recover the sum that was left in the recipient's account. I consider that the bank in effect did what they would normally do in such circumstances even where the payment had been made within the UK, and whether or not the payment was covered under the Code.

I know this will come as a disappointment to C. I am aware that they are strongly of the view that their bank let them down on this occasion. But I can only make an award against NatWest if I consider that the bank had done something wrong, which has led to C's loss. For the reasons given I am not persuaded that there was any error or omission on part of NatWest which has resulted in C's loss. As such I can't fairly or reasonably ask it to refund their loss.

C's response to my provisional decision

C did not accept my provisional decision. Their director gave a detailed response commenting on various parts of my decision all of which I have read and considered fully. In essence, they said:

The payment was made to someone C had paid in the past but this time purportedly to a new account of theirs. It was a large payment and to abroad. NatWest has past data from which it could have seen that this account was different to where C had paid the same

supplier in the past. So, it should have flagged a warning to C asking them to verify the account details with the supplier. This is especially as there was no recourse to the CRM Code for payments abroad.

My decision is inconsistent with a decision by another ombudsman in another case, as quoted in a magazine, which the ombudsman upheld where the circumstances appear to be similar.

It is incorrect to say that C would have proceeded with the payment in any case even if a warning was given. If the bank had warned C that they were at risk if a payment goes to a fraudster's bank account there would be no recourse (unless the money can be retrieved in time), then they would have made the payment by cheque.

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, I see no reason to depart from the conclusions I reached in my provisional decision.

I acknowledge the arguments presented by C. As the victim of a callous scam, I appreciate the director's strength of feeling on this matter and why they believe that the bank ought to have done more to prevent the scam. However, what I am considering here is whether it is fair and reasonable to conclude that the loss to C was caused by the bank.

It is not in dispute that the payment was authorised by C. The starting position in law therefore is that a bank is obliged to process the payments and withdrawals that its customer authorises it to make. But there can be circumstances where it might be appropriate for banks to take additional steps – as for example have systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud.

Ultimately, it is a matter for the bank as to how it chooses to configure its fraud detection systems and strike a balance between allowing its customers to transact business and questioning transactions to confirm they are legitimate. But where it is alleged that it didn't do enough to prevent a loss which resulted from an authorised push payment fraud, I will look into the circumstances of the case and based on what I have seen, decide whether in that case the bank could have fairly and reasonably done more.

I have considered this and for the reasons given in my provisional decision, I can't say that the disputed payment stood out sufficiently from the prior account activity to have prompted the bank take further action. I'm not persuaded that there was enough here for me to find the bank was at fault in carrying out C's payment instruction in line with its primary obligation to do so.

C says that NatWest had the data of past transactions from which it could have seen that the account to which C was making the relevant payment was different to where C had paid the same supplier in the past. So, it should have flagged a warning to C asking them to verify the account details with the supplier.

It is not unusual for a supplier to change their bank account details. So, it wouldn't automatically be a concern to the bank. Also in this instance, we have the bank statement for about a year prior to the relevant transaction and I can't find a prior payment to that supplier

during this whole period. So, it is not the case for example that the details were changed within days.

Nevertheless, as I said in my provisional decision, I agree that the bank could have given generic warning about scams and not having any recourse if the funds were lost. But I also said that in this instance it was more likely than not that C would have proceeded with the payment in any case.

C's director asserts that if such a warning was provided, the person who made the payment would not have proceeded with it.

If there is a dispute about what would have happened, I must decide on the balance of probabilities – in other words, what is most likely – in the light of the evidence.

In this instance, the director has explained that usually if C gets a specific request to change a bank account, they will contact the payee. But on this occasion, because the sub-contractor authorised the invoice, the person making the payment believed that the sub-contractor had also verified and ratified the change to the bank account. So, they did not deem it necessary to follow the usual procedure and verify the change with the payee and went ahead with the payment. In the circumstances, I remain of the view it is more likely than not that even if such a generic warning was presented to them when they made the payment, they would have proceeded with the payment as they had no doubt about the payment details.

The director has also referred to me an article in a magazine. He says that the circumstances of the case mentioned in that article appear similar to this case but in that case the ombudsman upheld the complaint. I am not aware of the specifics of the case and so cannot comment about it. However, the fact that the Service may arrive at different outcomes on separate cases should not be seen as surprising. It is not a question of inconsistency, but a matter of the ombudsman looking at each complaint individually and making a decision on what they believe is fair and reasonable in the circumstances of that particular case. There may be surface similarities between some complaints but when looked at in detail, the Service generally finds that different facts and issues are involved.

I am sorry to disappoint C. As I said earlier, what I am considering here is whether it is fair and reasonable to conclude that the loss to C was caused by the bank. For the reasons given I am not persuaded that was the case here. As such I can't fairly or reasonably ask it to refund their loss.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask C to accept or reject my decision before 12 January 2024.

Raj Varadarajan
Ombudsman