DRN-3952032

The complaint

Company A complains that National Westminster Bank Plc wouldn't reimburse the money they lost due to an authorised push payment scam.

What happened

The background to the complaint is known to both parties and so I won't repeat it at length here.

Briefly, as I understand it, in early 2020 the director of A, Mr D was cold contacted via email by someone claiming to be from Bank M, providing information about investment in shares. Following further discussions, Mr D agreed to invest in two corporate bonds.

During the third week of March 2020, the company made a payment of £300,000, purportedly for the first bond, to a beneficiary account with a bank, which I will refer to as 'H'. Then, between end of April and middle of May 2020, the company made multiple payments totalling £300,000 to a beneficiary account with an electronic money institution, which I will refer to as 'C'. This was purportedly for the second bond.

In August 2020, it came to light that these payments were made to a fraudster and the company was a victim to an elaborate investment scam.

On being advised of the scam, NatWest contacted H and C. Most of the payment made to H could be recovered but unfortunately C reported that none of the payments made to its customer could be recovered.

A made a claim to NatWest under the Contingent Reimbursement Model Code ('the CRM Code') for reimbursement of the money lost. NatWest initially said that the complaint wasn't covered by the CRM Code but on further representation from A, assessed the claim under the Code and agreed to reimburse 50% of the sum lost. This amounted to £152,529 (being 50% of £600,000 less £294,942 recovered from H).

Essentially, NatWest accepted that it could have done more to help prevent the fraud. The bank said that it spoke to A when three payments were made on 29 April, 3 May and 5 May 2020. It said the calls concentrated on confirming whether the payments were authorised but it could have done more by providing warning about investment scams. However, the bank only offered to reimburse 50% of the loss. It said that in accordance with paragraph ALL2(2)(b) of the Code, which at the relevant time, essentially stated that if the customer did not meet their 'requisite level of care' then each liable party will accept equal responsibility.

A did not agree. They said that none of the exceptions under R(2)(1) of the CRM Code applied and so they should not be asked to share any loss. In particular, they said that they did carry out due diligence prior to the investments which went far beyond the requisite level of care.

One of our investigators considered the complaint and concluded that NatWest should pay £25,000 in addition to what the bank had already offered. They said, in summary:

- It should first be decided whether A was a micro-enterprise at the relevant time. This is to decide whether the transactions are eligible to be considered under the CRM Code.

  A has said that their full-time equivalent staff number was 10, 10 and 8 for the years 2017, 2018 and 2019 respectively.

  Under our rules, for an enterprise to be considered as a micro-enterprise, the staff number should be less than 10, and the turnover or annual balance sheet should not exceed €2 million. In this instance the staff number was below 10 in the reference year (which was 2019). However, we need to look at the numbers across three consecutive years including 2019 and consider the status of A for two consecutive years of these three years.

  In this instance, the staff number was 10 for 2017 and 2018, and as such exceeded the requisite threshold for a micro-enterprise for two consecutive years. Therefore, the company could not be considered a micro-enterprise. This in turn means that the relevant transactions aren't eligible to be considered under the CRM Code.

- NatWest has accepted that it could have done more to help prevent the loss to A. So, it is fair that the bank compensates A.

  The bank however has said that both parties should accept equal responsibility in accordance with paragraph ALL2(2)(b) of the CRM Code. As the transactions aren't covered under the CRM Code, the arguments about the provisions of the CRM Code isn't relevant here. However, it is fair to consider whether A acted reasonably in the circumstances or whether they could have done more to prevent their loss.

- There was nothing suspicious about the email address from which the fraudster's emails came. Mr D says that when he spoke to the fraudster, he came across as "well-spoken and credible financial markets professional". The fraudster then sent various documents which looked genuine. Mr D has also said that he called the genuine Bank M and confirmed that the bank did have employees with the names stated on the emails. He also says that a leading consultancy firm that manages A's pension trust carried out its own due diligence before investing the trust money into identical schemes. So, this gave some added comfort to A.

  Taking all of the above into account, at the outset, A did what they reasonably could in the circumstances.

- However, by the time A made the second payment of £100,000 to C on 5 May 2020, there was enough going on that ought to have raised some concerns to A. Had A carried out some checks at the time, it is more likely that would have prompted them to carry out additional due diligence similar to what they did subsequently, and the fraud would have come to light. So, A missed an opportunity here to prevent their loss and therefore it is fair that they share the loss incurred, from this point onwards.

- As the bank has already offered 50% of the subsequent loss, it needn't do anything further in relation to those losses. However, it should refund a further £25,000 which would return the full first payment of £50,000 to A that was made prior to 5 May.

NatWest accepted the investigator's recommendation, but A didn't. They reiterated that they carried out all the necessary due diligence. They again pointed out to the fact that an external independent consultancy firm carried out their own due diligence and didn't find any concerns. They also didn't agree with the investigator that by the time A made the second payment of £100,000, there was enough going on to have raised some concerns to A.

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 agree with the investigator's conclusions essentially for the same reasons. However, I think that a small adjustment is needed in relation to the proposed redress. I will explain why.

I am thankful to A for providing detailed submissions to support the complaint, all of which I have read and considered in their entirety. However, I trust that they will not take the fact that my findings focus on what I consider to be the central issues, and that they are expressed in less detail, as a discourtesy. The purpose of my decision is not to address every point raised in detail, but to set out my conclusions and reasons for reaching them.

I agree that A's claim isn't eligible to be considered under the CRM Code, for the reasons given by the investigator. This in turn means that I don't have to specifically consider whether the provisions of the Code applied in this instance. That said, ultimately, I am required to decide the complaint by reference to what is, in my opinion, fair and reasonable in the circumstances of the case.

This is a sophisticated scam and I am sorry that A became a victim of it. NatWest has accepted that it could have done more to help prevent the loss to A. In particular, it has said that it could have done more when three of the payments were flagged on 29 April 2020, 3 May 2020 and 5 May 2020. It appears that there was no payment on 3 May but there was one on 4 May. Perhaps the bank is referring to this. In any case, the bank has acknowledged that on the occasions it called A, it should have provided investment scams advice to A, but it focussed only on confirming the payments were genuine and authorised.

After reviewing the submissions, I agree that the bank could have done more and so it is fair that it compensates A for the loss. The remaining question is whether A could have done more to prevent their loss.

I can see that at the outset, A did carry out some due diligence. Some of this appears to have been done by Mr D verbally over telephone. So, it is difficult for me to know for certain what exactly was discussed during those calls, but I have no reason to doubt Mr D's testimony in this regard.

Mr D has said that an independent professional consultancy services firm that manages A's pension trust carried out its own due diligence in relation to the trust, before investing the trust money into identical schemes. Though A is ultimately responsible for their own decisions, I accept that this would have given some comfort to A at the outset.

However, that is not the end of the matter. A was then asked to make the first payment to H. The beneficiary's name was different to that of Bank M. Mr D says he queried this with the fraudster, and he was told that the funds were being paid into intermediary accounts (owned and managed by Bank M). However, a quick search on the internet would have shown that

there was an entity with a similar name to that of the beneficiary, but it was different to Bank M.

Then, when it came to investing in the second bond, A was asked to send the money to an electronic money institution, to a completely different beneficiary account and name. Here again, the beneficiary name wasn't Bank M. A quick search would have shown that there is an entity with a similar name to that of the beneficary, but it is quite different to Bank M.

A went ahead and made a payment of £50,000. This payment was flagged by the bank and it contacted A to ensure that they are the ones who are making the payment.

Then, on the morning of 4 May 2020, A received an email from the fraudster asking them to make a further payment of £100,000 to the same account, with the same beneficiary's name in relation to the same bond. The company proceeded to make the payment and it appears that this payment too was flagged by the bank and once again they contacted A to ensure that they are the ones who are making the payment.

A then emailed the fraudster (thinking that they are emailing Bank M) to let them know that the payment was made as requested. The fraudster responded to say that they will update "immediately on clearance". There was no mention of any problem with the account at that time.

Despite the money being sent to the same account, the payment bounced. It is not clear why.

Mr D says that he contacted the fraudster following this and was told that this was due to "*a [Bank M] Capital account name error*". A was then asked to make the payment to the same account number again but with a slightly different beneficiary name.

Whilst a payment instruction may have included the name of the beneficiary, the unique identifiers are usually sort code and the account number. So, the payment would automatically be received into the account so long as those details were correct. So, I think the reason for the payment not going through being attributed to an error in the name was somewhat unusual. It should also be noted that when the payments were made, Confirmation of Payee - the name checking service - wasn't in place. So, there was no check to the payee name this way as well.

But even if A wasn't to know about what constitutes unique identifiers, only the day before 'Bank M' provided the previous details as correct. And later that day, after A made the payment and advised the 'bank' of this, it responded to say that it would update A on clearance.

I consider that a big bank like Bank M wouldn't usually have issues with its account name and even if it did, ought to be aware of any such issue as soon as it arose. But it seemed that the bank wasn't aware of the problem until A contacted it. I consider this too unusual.

Here again, a quick check would have shown that an entity exists matching the revised name but it is quite different not only to Bank M but also to the entity whose name was provided for the first payment.

I agree with the investigator that by this point there were enough indicators that ought to have caused some concern to A. They could no longer take what the fraudster said at the face value but ought to have paused and carried out additional checks.

As previously noted, a quick check would have shown that was no discernible link between Bank M and any of the named beneficiaries to whom A was asked to make payment to. Moreover, when Mr D ultimately became suspicious, he called the genuine bank again, but this time asked to be put through to the member of staff with whom he thought he was communicating, and the fraud came to light.

So, I consider that if A had done these before making the payment of £100,000, the fraud would have come to light sooner. I consider that A missed an opportunity here to prevent their loss and so it is fair that they share the loss incurred from this point onwards.

A has said that its pension trust also fell victim to the same scam and the trust's bank has reimbursed the amount in full. However, that does not automatically mean that is what should happen here too. What I consider to be fair outcome here depends on the specific circumstances of this complaint.

Putting things right

My finding is that the complaint should be upheld but A should share the loss equally with NatWest from the time the payment of £100,000 was made on 5 May 2020.

Prior to this payment, A had transferred £350,000 to the fraudster. Of this, as I understand it, £294,942 was already recovered from Bank H. This leaves A with a loss of £55,058. NatWest should reimburse A this loss.

From and including the £100,000 payment on 5 May 2020, the total loss to A was £250,000. This loss should be shared equally between NatWest and A. Therefore, NatWest should reimburse A £125,000 in relation to these payments.

Thus, NatWest should reimburse a total of £180,058 together with interest. Had the fraud not occurred, I consider it more likely that A would have reverted to keeping their money in cash or short-term investments with original maturities of three months or less, as they usually did. It is difficult to know now for certain what interest they would have earned on this sum had they done so. In the circumstances I consider it fair that NatWest pay interest on the above amount equivalent to the Bank of England base rate.

Interest should be paid from the date of the respective transactions that make up the £180,058 to the date of settlement. As I understand it, NatWest has already paid £152,529 to A in May 2021. So, interest on this sum should be calculated to the date of that payment.

My final decision

My final decision is that I uphold the complaint. In full and final settlement of it, National Westminster Bank Plc should pay in total £180,058 (including the sum it has already paid), plus interest as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask A to accept or reject my decision before 12 April 2023.

Raj Varadarajan
Ombudsman