DRN-5298947

The complaint

G, a limited company, complains that National Westminster Bank Plc won't reimburse them for their losses to an email intercept scam.

G has appointed professional representatives to handle this complaint. But for ease of reading, I'll only refer to G in this decision.

What happened

The background for this complaint is well known to both parties, and largely not in dispute. I will cover it only briefly here.

In December 2022 G's email system was compromised, and a fraudster sent several emails seemingly from the CEO asking for payments to be made to a new payee. Three payments were sent by G on the 22nd, 28th and 30th December before the ruse was discovered. In total G had sent £245,604 to the scammer.

G reported this to NatWest, who in turn contacts the receiving bank. But only £302.95 remained to be returned. G asked NatWest to reimburse them their remaining losses. However, the bank declined, saying that the payments were not out of character for the account, and that they had carried out the payment instructions as received. They said G's relationship manager wasn't specifically expected to provide them with scam awareness information but accepted that some of the service provided was poor. They offered £400 in compensation.

Dissatisfied with this G referred their complaint to our service. They felt the losses should be considered under the Lending Standards Board's Contingent Reimbursement Model (CRM).

Initially NatWest argued that G was too large a business for us to consider a complaint from, and that they had referred their complaint to us later than the deadline from the final response letter. But the investigator thought this was a complaint we could consider.

But our investigator thought that the CRM code didn't apply to G, because of the size of the business. The investigator thought that the transactions themselves weren't out of character for G's account, so it wouldn't be reasonable to expect NatWest to have intervened and asked further questions that would have revealed the scam. And they saw that NatWest's efforts to recover the funds were reasonable. Overall, they didn't feel that NatWest needed to do anything further.

G disagreed, arguing that the fact that the payments went to a new payee in such rapid succession should have prompted intervention by NatWest. They accepted that the CRM code did not apply to them but argued that this didn't absolve NatWest of their responsibility to detect and prevent scams. But this didn't change the investigator's mind.

As no agreement was reached, the complaint has been passed to me to decide.

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.

I see that previously NatWest has raised objections with our service about our jurisdiction to investigate this complaint, although they haven't advanced these points since our investigator's opinion that this was a complaint we can deal with. So, I have taken it as agreed that this is a complaint the falls within the remit of our service.

The transactions and the Payment Services Regulations

The relevant regulations here are the Payment Services Regulations 2017 (PSRs). These broadly say that the primary responsibility for the bank is to carry out legitimate payments instructions as quickly as possible.

In this case it's not disputed that the payments were made by individuals at G with the authority to transact of the account – so NatWest haven't done anything wrong by processing them. Once a payment transaction is duly authorised there is no requirement under the PSRs for NatWest to refund G. The starting position here is that G are liable for any losses. But I've also considered what's fair and reasonable in the circumstances, and whether NatWest should bear some of the losses.

Should NatWest done more to prevent the losses?

G have accepted that they are not covered by the CRM code – this is a voluntary code that says the banks signed up to scheme should refund losses to scams for consumers, charities, and micro-enterprises. But here as G had more than 10 employees at the time of the transactions it would not be considered a "micro-enterprise". So, I'm satisfied G is not covered by this scheme, or any of the considerations involved in deciding the outcome of a claim under the code.

Despite this, NatWest would still have an obligation to monitor accounts and payments transactions for signs of fraud or financial harm. If a particular payment, or sequence of payments, looks particularly egregious or out of place I may expect the bank to intervene, potentially by declining the payment request and asking further questions of the payer. The hope here is that any scam would be discovered.

There is a balance for NatWest to strike between security and allowing their customers to transact quickly and efficiently. Any intervention would need to be proportionate to the risk involved. And I also see it as reasonable that NatWest would expect a business the size of G to have their own systems and controls in place to mitigate any risks from fraud and scams.

I'm not persuaded that these three transactions stood out so significantly that NatWest would reasonably have been expected to intervene. Even putting aside payments clearly marked for salaries or tax, G's account had been used to make larger transactions. For example, the month previously payments of £180,000 and £350,000 had been made a day apart, to payees who weren't regular recipients of payments from G. And large business accounts, such as G's, by their very nature will be more likely to process larger value transactions than a personal or micro-enterprise accounts. Based on the previous account activity I'm not satisfied that payments of the amounts sent to the scammer should have been a particular concern to NatWest, even as a new payee.

The destination account name was confirmed through the Confirmation of Payee system, and the receiving bank has confirmed it was accurate. The payments didn't come close to

exhausting the balance of G's account. The third payment was authorised by a different individual at G than the first two, which would've suggested there was some wider knowledge of the payments at the time. And there aren't any other warning signals that would reasonably lead NatWest to conclude G was falling for a scam. I can't see there's a significant failing here by NatWest that ultimately means they should be responsible for G's losses.

Recovery of funds

G first reported the scam to NatWest on 3 January 2023. And I can see that they contacted the receiving bank within the hour to see if any funds remained. Unfortunately, they were only able to recover £302.50. But I see that NatWest acted within a reasonable timescale, and I'm not persuaded they could have done more to recover the funds.

Conclusions

I appreciate this will be a difficult conclusion for G – I've no doubt that they're the victim of a cruel scam, and this will have caused difficulty for the business and staff involved. I see that NatWest have offered £400 for service failings regarding the relationship manager. And this is reasonable.

But ultimately, I'm not persuaded that NatWest failed in their obligations to protect G's account in such a way that they should refund their scam losses. On that basis, I'm not asking NatWest to do anything further.

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 G to accept or reject my decision before 1 April 2025.

Thom Bennett
Ombudsman