DRN-4715675

The complaint

A partnership which I'll call 'R' complains that Clydesdale Bank Plc didn't reimburse them the money they transferred to a fraudster.

The complaint is brought on R's behalf by the partners, Mr and Mrs C.

What happened

The background to this complaint is well known to both parties so I won't repeat it all in detail here. But in summary I understand it to be as follows:

In December 2022, Mrs C received a 'WhatsApp' message from someone she believed to be her daughter, telling her that their phone had been damaged and they needed money to repair it. The message said that they'd been locked out of their bank account and asked that Mrs C reply to the phone number being used which was her daughter's temporary number. Mrs C says that it's not unusual for her daughter to ask for money by sending messages, so she didn't think this was odd and just replied to the message.

Throughout the rest of the day, the messages continued, and Mrs C was asked to help her daughter make payments towards the phone repair, insurance, and security deposit. Believing everything to be genuine, Mrs C made a number of payments to different accounts thinking that she was helping her daughter. During this period, Mrs C was also told that some of these payments – as the security deposit – would be returned.

Mrs C was told to log into her banking app, and make various payments. She was advised that this would verify her identity with the phone shop after which the payments would be returned. She was also told that Clydesdale would be contacting her to verify the largest payment. But unfortunately, she was messaging the fraudsters impersonating her daughter and had been sending money to the accounts they controlled.

Throughout the day, Mrs C made two payments to a new payee from her personal account totalling £1.280. Alongside this Mrs C said that she gave the fraudsters her card details, and they took two further payments totalling about £2,500. Mrs C then made a further four payments from R's business account totalling about £31,000 to two new payees. Mrs C was then told that her daughter could collect the phone and that she would receive a refund at midnight of the security payments that she'd made. Mrs C said she continued to receive reassuring messages from the fraudsters until around 23:00. At 23:30 she called her daughters real phone number, following which the scam came to light.

Mrs C subsequently contacted the police and Clydesdale. Clydesdale refunded the transactions from Mrs C's personal account under the Contingent Reimbursement Model Code ('the CRM Code'), but it declined to refund the payments from R's business account. It said that Mrs C didn't have a reasonable basis for belief when making these payments. It therefore said that an exception applied in this case.

Our investigator recommended the complaint be upheld, and for Clydesdale to refund 50% of R's losses. He thought that some of the messages from the fraudster, lack of contact from

the insurance company, and the high value amounts being requested for phone insurance, should have alerted Mrs C that something wasn't quite right and therefore she should take some responsibility for the loss. However, the investigator didn't think that Clydesdale's warning was effective when Mrs C had made the payments from R's account. He also thought that the bank should've done more as the payments were unusual for the account.

Both Mrs C and Clydesdale disagreed with the investigator's opinion, so 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.

In deciding what's fair and reasonable, I'm required to consider relevant law and regulations; regulatory rules, guidance, and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

Where the evidence is incomplete, inconclusive, or contradictory (as some of it is here), I reach my decision on the balance of probabilities – in other words, on what I consider is most likely to have happened in light of the available evidence and the wider circumstances.

Clydesdale is a signatory of the Lending Standards Board Contingent Reimbursement Model CRM Code (CRM Code) which requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. Clydesdale says one or more of those exceptions applies in this case. The exceptions relevant to this case are:

- The customer made the payment without a reasonable basis for believing that: the payee was the person the customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate.

- The customer ignored an effective warning in relation to the payment being made.

There are further exceptions within the CRM Code, but they don't apply in this case.

The CRM Code also outlines the standards a firm is expected to meet. And it says that when assessing whether the firm has met those standards, consideration must be given to whether compliance with those standards would have had a material effect on preventing the APP scam that took place.

So, when considering this complaint, I need to look at the actions of both Mrs C, as the person making the payments and Clydesdale as the bank facilitating the payments, and whether either or both could have done more to prevent the loss(es) involved.

Reasonable basis for belief

Clydesdale say that it doesn't think it should reimburse R under the CRM code as Mrs C didn't have a reasonable basis for belief. When looking at this case, I need to consider not just whether Mrs C believed she was sending money to her daughter, but also if it was reasonable for her to do so. So, I've thought about what Mrs C did when deciding to send the payments and whether that was reasonable. The first thing I've considered is that Mrs C thought she was sending payments to her daughter. I think the initial contact with the fraudster was plausible to Mrs C's personal situation. In this regard, please note that the first

four transactions from Mrs C's personal account do not form part of this decision as they have been refunded, however I have referred to them as context for the transactions from R's account.

Mrs C told us that it wasn't uncommon for her daughter to ask for money when needed, and it's understandable that Mrs C, as a parent, wanted to resolve her daughter's problem as quickly as possible. Mrs C was told that her 'daughter's' phone had been dropped in water, so it wasn't working - and therefore she couldn't access her own bank details. Mrs C was asked to transfer £640 directly to the phone shop. I think this seems reasonable based on the cost of a mobile phone and the situation the fraudster said had taken place. Furthermore, given that the fraudster also said the phone was broken, I think the explanation about messages from another phone also seems reasonable.

Mrs C received a further text message around an hour later which asked her to send a further £640. Mrs C questioned this payment but was told this was needed as a security deposit, as there was insurance on the phone. Mrs C was then told she would receive both payments back due to the insurance. I think the reason for the additional payment was plausible and in line with the situation Mrs C thought her daughter was in.

Shortly after making the second payment, Mrs C was asked to provide her account details which the payment had been made from – which she did. However, the fraudster said it was the card details that were needed, and requested screen shots of the front and back of the card. Even if Mrs C didn't think that the request was unusual, the fraudster then asked for Mrs C's postcode. I think it's likely that her daughter would have known this information.

Then, around an hour later, Mrs C received a further text asking her to authorise more payments. And at that point Mrs C saw that two payments for £1,003 and £1,504.50 which she hadn't made had been taken from her account. The fraudster said this was firstly as a security deposit and then to make sure there was sufficient funds in the account. They then said that this money would be refunded within the next 10 minutes.

Around 90 mins later, Mrs C messaged the fraudster questioning why the funds hadn't been paid into her account. She also tried to call her daughter's new number, but the call was cancelled by the fraudster – who explained that they (still pretending to be her daughter) couldn't take calls. There was then a discussion about a further £1,000 payment, insufficient funds in the account and that refund hadn't been received. At this point, the fraudster told Mrs C that they needed a further £4,000 payment. Mrs C didn't query why they needed a further £4,000 but, she simply told them of the significant balance that was held within R's account.

Mrs C then messaged the fraudster to say that £1,021.80 had been received into R's account as a refund instead of her personal account. R's statements don't show any evidence of the payment – but I have no reason to doubt what she communicated to the fraudster at that time.

Mrs C was then asked to send a further £3,787 to the 'phone shop's insurer', and was told that she would receive a refund from the phone shop once this had been confirmed. But the payment details she was given were for an individual. Mrs C said she was confused by this but was told this was so that the system could confirm she had authorised the payments and that this was a 'relay refund' which was totally normal. It appears that Mrs C was sceptical at this point and said that these payments were a lot for a phone. Following this, the fraudster's story changed, and she was told that this payment was for Christmas Presents and they had been given a large discount which they wanted to utilise.

I think that by now, there were enough inconsistencies and unusual requests that ought

reasonably to have alerted Mrs C that something wasn't quite right. I don't think she had reason to think this could be an amount related to a damaged phone. I say this because, even if upfront costs were needed to be paid to an insurance company, Mrs C had already made payments for significantly more than a mobile phone's value at this point.

Mrs C then made the £3,787 payment to the 'insurer' from R's account as instructed and within around five minutes, the account received a refund of the same amount from the 'insurer'. This was purportedly to reassure Mrs C that the business she was dealing with were legitimate.

Mrs C remained concerned about the money she had already transferred and messaged the fraudster to request the refund of the £3,787 (the total of the four payments) to her personal account as she had now made transfers totalling £7,574. This wasn't done, but Mrs C was asked to send a further £10,000 as a 'security deposit'. This was to a different payee in the name of a computer company, not the individual who was supposedly the insurer and who had made the refund.

Mrs C told us that she was confused at this point and didn't really want to make the next payment, but was reassured when she received the first £3,787 back from the fraudster. I appreciate what Mrs C says, but a request for such a large deposit for the repair of a mobile phone wasn't a reasonable request. It also wasn't consistent with the original reason that that fraudster had given her for needing funds to be transferred.

Mrs C says that she was then told she'd receive a call from Clydesdale to verify the payments. Shortly after, she received a call from who she thought was the bank. Mrs C says she was then told to make a further payment of £13,787 as a 'security deposit' by her bank (in the case the fraudster assuming Clydesdale's identity). Mrs C says that she thought this was legitimate as how would anyone else have known who her bank was. But I think Mrs C ought to have cause for concern that her daughter would know in advance that Clydesdale would be calling her, and that 'the bank' instructed her to make a payment to a new payee, and for the same transaction amount that totalled the two earlier payments she'd made that day.

I have considered all of the above. In my view, as I have said earlier, by the time Mrs C was asked to send the £3,787 there was enough going on that Mrs C should've had concerns and taken further steps before she made the payment(s). So, I can't fairly say that she met the requirements under the Code from this point on.

I acknowledge that Mrs C says she was put in a vulnerable position, and she feels she's being penalised for being the victim of a scam. But overall, I don't think Mrs C had sufficient reason to disregard some of the clearer warning signs here.

Effective warnings

The CRM code says that with regards to APP scams that a business sending fund should provide an effective warning to its customers. Section SF2 (2)(c) says that "Effective Warnings should be risk based and, where possible, tailored to the APP scam risk indicators and any specific APP scam types identified through the user interface with which the Customer is initiating the payment instructions." What this means in practice is that a warning should be understandable, clear, impactful, timely and specific.

In this case, I'm satisfied that the requirements of the effective warning exception were not met because don't think that the warning was effective here.

Clydesdale told us that the warning presented to Mrs C was the same for all the payments.

The warning said "*Fraudsters can pretend to be from a company you know to trick you into paying the bill. Check you got the account details from a trusted phone number or person. You had time to pay without pressure or threat of penalties. And the bill wasn't unexpected*."

I think the warning was timely, in that Clydesdale say it was presented at the time of the transfers. However, I don't think the warning was meaningful or clear to Mrs C as it didn't represent any similarities to the payment that she was making. The payment request did not come from a company about paying a bill. And it came from a trusted person (or so she thought) for a different reason.

So, I don't think the warning given by Clydesdale was impactful, nor was it specific or clear to Mrs C that the transactions she was undertaking were part of a scam, particularly because as far as she was concerned, the payments were for a phone and were deposits which would be returned – not bill payments.

Actions taken by Clydesdale

As I noted earlier, I don't think Clydesdale provided an effective warning. In addition, I think that Clydesdale ought to have intervened after the second payment from R's account, i.e., at least after the payment of £3,787 was made.

I say this because the first payment (£3,787), although a little higher than normal, wasn't out of character for the account. However, the £10,000 and £13,787 were both unusual amounts compared to the normal account activity. In addition, they were made within a short time period and to a new account payee.

Clydesdale says that the payments were no unusual. I've looked at R's bank statements and see that there weren't payments over around £5,000 from the company's account – and the payments of that size were direct debit payments and to recognised entities such as HMRC or suppliers. So, I think Clydesdale out reasonably to have identified that these transactions were out of character for R's account. And I think that if Clydesdale had intervened and contacted Mrs C, at least when the payment of £10,000 was attempted to ascertain what was going on, the fraud would have come to light and the losses from R's account from that point on would have been prevented.

I've also thought about whether Clydesdale took reasonable steps to recover R's funds, once it was aware that Mrs C had been the victim of a scam, and I'm satisfied that it did.

However, I've also seen that although Clydesdale did keep in contact with Mrs C at various points to discuss the circumstances of the complaint, it took until mid-March 2023 for the bank to provide her with a response. This caused R inconvenience as Mrs C had to keep chasing the bank at what was already a difficult time for her from the realisation that she'd lost funds from the partnership's account. That being said, I can see that Clydesdale has apologised for the poor service and paid Mrs C £200 compensation for the inconvenience caused. So, I think it's done enough with this part of the partnership's complaint right.

I'm sorry to disappoint Mrs C as I know she wanted all of the funds lost to the fraudster refunded. However, based on all the circumstances of the complaint, I think both Mrs C and Clydesdale bear equal responsibility for the losses caused to R. Therefore, I'm recommending that Clydesdale refund 50% of the £23,787 losses the partnership incurred as a result of the £10,000, and £13,787 payments.

So, in summary, I don't have to decide on the first four transactions from Mrs C's personal account as they have been refunded and in any case were not made from the complainant's (R's) account. By the time Mrs C made the first payment of £3,787 out of R's account, there

was enough going on that she should've had concerns and taken further steps before she made this and the subsequent payments of £10,000 and £13,787. That said, as previously noted, the fraudster has refunded the £3,787.

On the other hand, I consider that Clydesdale ought to have intervened at least when Mrs C made the payment of £10,000. In addition, I don't think its warning was effective.

Therefore, I consider it fair that Clydesdale reimburses 50% of the loss incurred by R starting with the payment of £10,000, i.e., 50% of £23,787. Clydesdale should also pay interest on this amount at 8% simple per annum. Interest should be paid from the date of the payments to the date of settlement.

My final decision

My final decision is that I uphold this complaint. In full and final settlement of it, Clydesdale Bank Plc should:

- Refund R 50% of £23,787.
- Pay interest at 8% simple on the above amount from the date of the payments to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask R to accept or reject my decision before 25 April 2024.

Jenny Lomax
Ombudsman