DRN-4246966

The complaint

Miss C complains that Lloyds Bank Plc didn't do enough to protect her from the financial harm caused by an investment scam company, or to help her recover the money once she'd reported the scam.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Miss C came across an online advertisement for a company I'll refer to as "S". The advert said that if she invested £250, she would double her money. The advert contained case studies of people who had made money and stipulated that S would use their expertise to make trades on commodities and cryptocurrency.

Miss C felt this seemed like a plausible way to save for a house deposit, so she clicked on the link and was redirected to an enquiry form, which she completed. The next day, she was contacted by someone claiming to be a broker working for S who explained he would make trades in cryptocurrency on her behalf. She was told to set up an online account and send documents regarding her immigration status.

She made an initial investment of £249.87 on 17 December 2021 but the next day, she contacted Lloyds to ask it to withhold the initial payment as she was worried about the immigration documents she'd sent and was concerned that she'd been scammed. The call handler told Miss C to ask S for a refund and said it could investigate the payment if they refused. They also told Miss C to be wary of scams in the future and not to send any more money if she believed she was being scammed.

When Miss C spoke to the broker, he told her it was standard procedure to ask for ID documents. He apologised for getting off on the wrong foot and said that if she wasn't satisfied with her profit over the next two weeks, he would recover the money and close her account. He told her he'd worked in finance for over 10 years and that his commission rate would vary. He told her to download AnyDesk so she could see her trades, leaving her feeling confident that S was legitimate.

The broker told Miss C she would need to invest more and advised her to take out a loan, which he did remotely on her behalf, declaring it was for 'home improvements'. He also advised her to open an account with "T" so she could convert her money cryptocurrency before sending it to an online wallet.

On 13 January 2022, Miss C made a payment of £10,000 to T and within a few days she could see her account balance had increased to £13,500. But on the seventh day the broker told her there had been a crash and her account balance had fallen to £200. At this point he told her he'd assign her to a senior broker who advised her to invest more to compensate for the crash.

But when she tried to make a further payment, it was blocked. During the call, Miss C was open about the circumstances of the payment and was advised not to send the money. At this point she realised she was the victim of a scam and contacted Lloyds.

Lloyds didn't agree to refund the money she'd lost. It said she'd been promised unrealistic returns and she should have done more checks before going ahead with the investment. It said the FCA had issued a warning about S on 20 October 2021 which was last updated on the 29 November 2021, and there were negative reviews online about S which were posted before she invested.

It said it didn't contact Miss C when she made the £10,000 payment because it was to an account in her own name. And as there was no mention of S during the call that took place in December 2021, it's advice to contact the recipient bank on that occasion was correct.

Miss C complained to this service with the assistance of a representative. They said Lloyds had failed to provide a sufficient warning when she tried to make the first payment and had missed a chance to make basic enquires, ask probing questions and engage with her as to why she was making such payments. Further it said Lloyds had actually initiated contact between Miss C and the scammer which caused her further financial harm and that if the call handler had conducted a search, they would have realised there was an FCA warning posted about S on 20 October 2021.

They also said that Lloyds had contacted her on 13 January 2022 when she made the £10,000 payment and its staff should have known that scammers groom their victims to give false accounts. They also said it should have probed further when understanding why Miss C needed to send money to T for home improvements. They argued Lloyds should have asked why she'd taken out a loan with an external company, why she was using T if the payment was for home improvements, and whether she was under pressure to make the payment.

They said that if Lloyds had asked more probing questions, it would have realised Miss C was falling victim to an investment scam, even though she was sending money to a legitimate cryptocurrency exchange company. And it should have provided a scam warning in light of all the information known to banks about the increasing number of scams associated with scammers selling what is made out to be cryptocurrency.

They explained the activity was unusual for Miss C's account and the high value payments to new payees relating to cryptocurrency should have been immediate red flags and it should have intervened when she made the £10,000 payment. They said the account was subject to a high influx of personal loans equating to £10,000 which were then forwarded to the scammer, and this rapid movement of borrowed funds should have been a cause of concern.

NatWest maintained there was no mention of S during the call that took place in December 2021 and Miss C didn't provide any information that would have led it to believe she was the victim of a scam. It said it allowed the £10,000 transaction to be processed without further intervention because it was to an account in Miss C's own name and she had willingly opened the account and provided full identification, so it wouldn't have been expected to intercept the payment.

Our investigator initially said the complaint should be upheld in part. He explained the CRM code didn't apply as these were payments to account Miss C held in her own name, and that there was no prospect of a successful chargeback for the same reason.

He didn't think the payment of £249.87 was suspicious or unusual. He accepted Miss C had contacted Lloyds after she made the payment, but it was given the impression she was more unhappy with the service she'd received and he didn't think she'd been led to believe S wasn't operating a scam.

But he thought Lloyds should have contacted Miss C on 13 January 2022 when she made the £10,000 payment and that any questions about whether anyone else was involved would've stopped the scam, as she likely would have told the truth if she was asked appropriate questions and she didn't go ahead when Lloyds intervened when she tried to make the final payment. But he thought the settlement should be reduced by 50% for contributory negligence because she could have prevented her own loss had she done adequate checks and read the FCA's warning about 'S'.

Lloyds didn't agree with the outcome. It said it didn't intervene on 13 January 2022, but Miss C had said she'd spoken to someone about the £10,000 payment, meaning it must have been stopped by T when she moved it on to the scammer. It said her own account is that there was a call during which she said the payment was for home improvements and so, if it had asked the same question, she'd have given the same response, and the payment would have been processed.

Our investigator issued a second view in which he explained Lloyds should have flagged and questioned Miss C about the £10,000 payment, but he didn't think it would have made any difference to her decision to go ahead with the payment. He explained both parties agree it's possible the payment was blocked by T and that Miss C says she explained the payment was for home improvements, because she was instructed to lie by the broker. So, he was satisfied that even if Lloyds had asked her about payment, it's likely she would've said it was for home improvements and it wouldn't have been able to detect the scam.

Miss C's representative has asked for the complaint to be reviewed by an Ombudsman. They pointed out our investigator previously relied on the fact Miss C did cease to make payments following adequate intervention when she tried to make the final payment, which is evidence she stopped making payments once Lloyds intervened.

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've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Miss C has been the victim of a cruel scam. I know she feels strongly about this complaint and this will come as a disappointment to her, so I'll explain why.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Miss C says she'd fallen victim to, in all but a limited number of circumstances. Lloyds had said the CRM code didn't apply in this case because the disputed payment was to an account in Miss C's own name, and I'm satisfied that's fair.

I'm satisfied Miss C 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, Miss C is presumed liable for the loss in the first instance.

I've carefully considered the circumstances, and I am persuaded the broker was operating as part of a scam. But, although Miss C didn't intend her money to go to scammers, she did authorise the disputed payments. Lloyds is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

I've thought about whether Lloyds could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange company. However, Lloyds had an obligation to be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have done more to warn Miss C when she tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Lloyds to intervene with a view to protecting Miss C from financial harm due to fraud.

The first payment didn't flag as suspicious but Miss C contacted Lloyds the following day and so it did have an opportunity to intervene at that point. Lloyds told her to contact the recipient bank and gave a generic fraud warning. I've considered whether it did enough at that point, and I'm satisfied that it did. The payment was low value, it was to an account in her name and there was no mention of S, so don't think it was unusual or suspicious, therefore I don't think Lloyds needed to have done anything more than it did at that point.

I've considered the nature of the second payment in the context of whether it was unusual or uncharacteristic of how Miss C normally ran her account and I think it was. Lloyds has argued the money was transferred to an account in Miss C's name but based on the value of the payment and the fact it related to cryptocurrency, I think it should have blocked the payment and contacted her to ask questions around the circumstances of the payment.

But Miss C has said there was a call when she tried to make the payment and that she told the call handler she wasn't pressured to make the payment and that it was for home improvements. The call agent her gave a general fraud warning and the payment was processed. Having carefully considered the evidence and the circumstances, I think it's most likely this is a recollection of a call Miss C had with T, and it's likely she'd have given similar responses to questions if Lloyds had intervened. And, based on the fact Miss C would probably have told Lloyds she wasn't pressured to make the payment and it was for home improvements, I think it's likely the payment would have been processed, even if Lloyds had blocked it.

Miss C's representative has argued that she listened and acted on the advice she was given by Lloyds when she tried to make the final payment and I accept this might be indicative of how she would have responded to an effective warning. But matters had progressed by that point and I think the way she responded to T's questions on 13 January 2022 is most relevant to what she would likely have done on the same date if Lloyds had intervened. So, I don't think Lloyds failure to intervene on 13 January 2022 represents a missed opportunity to have prevented her loss and I can't fairly ask it to do anything further.

Chargeback

I've thought about whether Lloyds could have done more to recover the first payment when she reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Lloyds) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Miss C).

Miss C's own testimony supports that she used cryptocurrency exchanges to facilitate the transfers. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Miss C's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Lloyds's decision not to raise a chargeback request against the cryptocurrency exchange company was fair.

I'm sorry to hear Miss C has lost money and the effect this has had on her. But for the reasons I've explained, I don't think Lloyds could have prevented this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decisionYour text here

For the reasons I've outlined above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss C to accept or reject my decision before 10 October 2023.

Carolyn Bonnell
Ombudsman