DRN-4526586

The complaint

Mr G complains that National Westminster Bank Plc trading as Ulster Bank didn't do enough to protect him from the financial harm caused by an investment scam company, or to help him recover the money once he'd reported the scam to it.

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.

In May 2022 Mr G met someone on social media who I'll refer to as "the scammer". They engaged in a few messages on the platform before exchanging numbers and communicating via WhatsApp. Mr G began to build a friendship with the scammer, exchanging photographs, videos and voice notes, and the scammer said he worked in data and was into investments.

The scammer told Mr G he was making a lot of money through trading in cryptocurrency and that he used an investment platform I'll refer to as "D". He said he would teach him how to invest and that he wanted to share the joy of trading with him. Mr G started to worry that he was pushing the scammer away, so he agreed to invest.

The scammer told him to first purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto an online wallet. He told him to open an account with a cryptocurrency exchange company and that he needed to buy £100 USDT, which would generate a daily profit.

Between 13 May 2022 and 20 June 2022, he made 12 transfers totalling £12,999.94 from his Ulster account. The initial investment of £50 on 13 May 2022 was blocked by Ulster and during the subsequent call, Mr G was asked what the payment was for, and the payment was released. Over the next 17 days, Mr G made six payments totalling £2,499.94, after which the scammer persuaded him to upgrade his trading account to the gold package, which meant that he would get a higher return. He was then asked to transfer £10,000 to meet the deposit requirement, but as he didn't have the money, he asked if the scammer to lend him £1,900.

On 20 June 2022 Mr G was told his account was frozen and he needed to transfer £3,000 to unfreeze the account. He asked the scammer for help but he refused and so he made two payments to cover the amount due. He realised he'd been scammed when the scammer stopped replying and he could no longer access the trading platform.

Mr G complained to Ulster arguing it had failed to flag the payments as suspicious, but it refused to refund any of the money he'd lost. It said it had acted on Mr G's genuine instructions to process the payments and all the payments were sent to an account in Mr G's own name before being transferred. It also said wasn't the point of the loss, so he would need to complain to the cryptocurrency exchange company he paid, and he had failed to carry out due diligence on the scammer or to take appropriate care when using the cryptocurrency wallet.

Ulster further explained it placed appropriate and relevant warning messages across its online banking facility to warn customers about scams and information is made available on its websites and within its branches. Warnings are displayed before making a transfer or adding a new payee and a tailored scam warning is displayed, requiring customers to confirm they are confident they have read and understood the advice and they are satisfied they have taken relevant steps.

It said if Mr G had followed the advice, he wouldn't have fallen victim to the scam and the payments were genuinely made using his secure online banking facility and there were no concerns at that time on the validity of the payments.

It said that as the payments were made to an account in Mr G's name, the CRM code wouldn't apply and it acknowledged he had vulnerabilities, but it didn't accept there was any reason why he wouldn't have been able to avoid being the victim to a scam.

Mr G wasn't satisfied and so he complained to this service with the assistance of a representative. He said he thought the investment was genuine, having received no effective warning or advice from Ulster and he wouldn't have gone ahead with the payments if he knew the investment could be a scam. He also said he was susceptible to scams and this should have been considered as a part of the investigation.

Mr G's representative said Ulster should have intervened as Mr G made 12 payments to a new payee linked to cryptocurrency within the space of 37 days and it should have intervened to protect him. They said the pop-up warnings were not specific so they couldn't be considered effective.

They noted Ulster had identified the first payment as unusual and contacted Mr G to confirm he was making the payment, which was an opportunity to ask relevant questions to determine the true nature of the payments. They also said it should have intervened when he made the later payments which were for larger amounts and if it had asked relevant questions, it would have been apparent that he was falling victim to a scam.

Specifically, it should have asked him where he came across the opportunity, whether there was a third party involved, whether he'd done any research, whether he'd been promised unrealistic returns and whether he'd received any withdrawals and that it's likely he would have fully explained what he was doing and that everything had originated from a broker.

They said Mr G wasn't prompted to give false answers and so Ulster should have realised he the investment had the typical hallmarks a scam.

My provisional findings

I explained that the CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr G says he's fallen victim to, in all but a limited number of circumstances. Ulster had said the CRM code didn't apply in this case because Mr G paid an account in his own name, and I was satisfied that was fair and applies to all the four bank transfer payments.

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

I explained there's no dispute that this was a scam, but although Mr G didn't intend his money to go to scammers, he did authorise the disputed payments. Ulster 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 thought about whether Ulster could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I'd seen, the payments were made to a genuine cryptocurrency exchange company. However, Ulster had an obligation to be alert to fraud and scams and these payments were part of a wider scam, so I needed to consider whether it ought to have intervened to warn Mr G when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Ulster to intervene with a view to protecting Mr G from financial harm due to fraud.

The payments didn't flag as suspicious on Ulster's systems. This was a new account and so there was no spending history to compare the payments with, but I agreed with our investigator that the first nine payments were low value payments to a legitimate cryptocurrency exchange and so they weren't unusual for the account. However, I noted that on 1 June 2022, Mr G made a payment of £5,000 and, based on the fact this was a high value payment to a cryptocurrency merchant, I thought Ulster should have intervened.

During the call, Mr G should have been asked questions around the purpose of the payments, whether there was a third party involved and, if so, how he'd met the third party, whether he'd been promised unrealistic returns, whether he'd been told to download remote access software to his device and whether he'd been told to make an onwards payment from the cryptocurrency exchange. And as there's no evidence that he'd been coached to lie, I was satisfied Ulster would have had enough information to identify that he was being scammed.

I said I would then expect Ulster to have warned Mr G about the risks associated with the investment and to have explained that there were red flags present including the fact he was taking investment advice from someone he'd met on social media and that he'd been told to make an onwards payment from the cryptocurrency exchange. I'd also expect it to discuss with him the nature of the checks he'd undertaken and to give some advice on additional due diligence.

There were no warnings about D on either the Financial Conduct Authority ("FCA") or International Organisation of Securities Commissions ("IOCSO") websites which would have alerted Mr G to the fact there was a scam. But I hadn't seen any evidence that he was keen to take risks and he didn't have a history of high-risk investing, so I thought that if he'd had any inkling this might be a scam, it's unlikely he'd have gone ahead with any more payments.

Consequently, I thought Ulster missed an opportunity to intervene in circumstances when to do so might have prevented Mr G's loss and I was minded to direct it to refund the money he lost from 1 June 2022 onwards.

Contributory negligence

I explained there's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence. Mr G had said he researched D and that he also contacted the cryptocurrency exchange company who told him it looked like a genuine company. He also explained that he hadn't invested in cryptocurrency before, so this was an area with which he was unfamiliar, so he wouldn't have known the returns were unrealistic or how to check the information he'd been given.

This unfamiliarity was compounded by the sophisticated nature of the scam, the fact he believed he could see his profits on the trading platform and the fact he believed he'd built a genuine friendship with the scammer. So, while I accepted Mr G shouldn't have taken investment advice from some he met online, in the circumstances, I didn't think he could fairly be held responsible for his own loss.

Compensation

I explained Mr G was unhappy that Ulster refused to refund the money he lost to the scam, but Ulster isn't responsible for the distress and inconvenience he suffered, so he isn't entitled to any compensation or legal costs.

Developments

Ulster has clarified that the final three payments took place on 17 June 2022 (£1,000),19 June 2022 (£2,000), and 20th June 2022 (£5,000).

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 accept the final three payments happened on 17 June 2022, 19 June 2022, and 20 June 2022 and not 1 June 2022, 20 June 2022, and 20 June 2022 as I have said in my provisional decision.

I maintain that Ulster should have intervened when Mr G made the £5,000 payment, but as this was the final payment, it only needs to refund this amount.

Ulster hasn't made any comments which relate to contributory negligence and so I remain satisfied that whilst there may be cases where a reduction for contributory negligence is appropriate, I don't think this is one of them.

My final decision

My final decision is that National Westminster Bank Plc trading as Ulster Bank should:

- Refund Mr G £5,000.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If National Westminster Bank Plc trading as Ulster Bank deducts tax in relation to the interest element of this award it should provide Mr G with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr G to accept or reject my decision before 17 January 2024.

Carolyn Bonnell
Ombudsman