DRN-4372300

The complaint

Mrs H complains that Nationwide Building Society 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 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.

Around 14 years ago, Mrs H invested around £500 in cryptocurrency. Unfortunately, she didn't hear anything back from the investment and has never invested in cryptocurrency since.

In January 2022 she was contacted by someone I'll refer to as "the scammer". The scammer said he was from an investment company I'll refer to as "B", they had located money in an account in her name and the initial investment had grown. Mrs H researched B and was reassured by the genuine-looking website and the reviews she saw on TrustPilot.

The scammer explained that they had located her cryptocurrency wallet but because it had been inactive for a number of years, she would need to pay B to reopen her account. He advised her to open an account with B and to download AnyDesk remote access software to her device. He also told her to open an account with an EMI I'll refer to as "W" and required her to send copies of her ID to prove she was the owner of the initial investment.

To make the payments, the broker asked Mrs H to first purchase cryptocurrency through a cryptocurrency exchange company and then load it onto an online wallet. On 19 August 2022, she paid £548, £560, and £6,420 to the account she'd opened with W.

When Mrs H told the scammer she didn't have any more money to send, he said her funds wouldn't be released and began ignoring her calls and messages. Mrs H realised she'd been scammed when she eventually lost touch with the scammer. She complained to Nationwide, but it refused to refund and of the money she'd lost apart from £10 that it had been able to recover from the recipient account. It suggested she should contact W because the funds were lost from that account.

Mrs H wasn't satisfied and so she complained to this service. She said Nationwide didn't intervene when she made the payments, and she didn't receive any warnings about the risks of investment scams. She said there were clear red flags such as multiple payments on the same day to a new payee linked to cryptocurrency, causing a rapid depletion of funds.

Her representative said the payments represented a sudden increase in spending and the payments were all made on the same day. They argued that if Nationwide had contacted Mrs H when she made the first payment, it could have prevented her loss. They said Nationwide should have asked Mrs H why she was making the payment, who she was trading with, how she found out about the company, whether she'd done any research, whether she'd checked the Financial Conduct Authority ("FCA") website, whether she'd been

promised unrealistic returns and whether she'd received any withdrawals. And had it done so, as Mrs H wasn't prompted to give false answers, she would have told it she was making payments for the release of funds from an investment she made over 14 years ago and it would have realised she was falling victim to advance fee scam.

Our investigator felt the complaint should be upheld. He explained that Mrs H's normal account activity generally consisted of lower value payments, so he thought the third payment on 19 August 2022 should have been flagged. He was satisfied that if Nationwide had contacted Mrs H and asked her why she was making the payments it would have learned she'd been asked to send funds to recover lost cryptocurrency and that she'd been asked to download AnyDesk, and it would have been obvious that she'd been scammed. Nationwide should then have provided an appropriate warning which he thought Mrs H would have acted on.

He thought Nationwide should refund the money she'd lost from the third payment onwards and he didn't think the settlement should be reduced for contributory negligence because the scammer had said they were from a reputable trading platform and Mrs H had completed due diligence before sending these funds.

Nationwide has asked for the complaint to be reviewed by an Ombudsman. It has said 'me-to-me' payments aren't covered by the Contingent Reimbursement Model ("CRM") Code and has suggested the onus was on W to intervene because the funds were transferred to the scammer from that account.

It has said the outcome is at odds with our approach to other 'me-to-me' scam cases, where we have said that a payment between customer's accounts didn't cause or give rise to a loss prior to the onward payment to the scammer. It has also said that our investigator has applied the same approach as 'me to me' scam cases involving payments to cryptocurrency merchants, which aren't regulated by the FCA. It has argued that permitting payments to a cryptocurrency exchange has visibility that it is a cryptocurrency transaction, whereas it had no knowledge of the onward payments from W.

It has also argued there was a break in the chain of causation as W could still have prevented Mrs H's loss and should be regarded as the operative cause of the loss, which is an established principle of causation. And it has suggested that if the case was decided in court, it would been entitled to seek a full contribution from W.

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.

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

I'm also satisfied Mrs H '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 her bank account, Mrs H is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mrs H didn't intend her money to go to scammers, she did authorise the disputed payments. Nationwide 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 Nationwide could have done more to prevent the scam from occurring altogether. Nationwide ought to fairly and reasonably 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 intervened to warn Mrs H when she tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Nationwide to intervene with a view to protecting Mrs H from financial harm due to fraud.

The payments didn't flag as suspicious on Nationwide's systems. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mrs H normally ran her account and I think they were. The first two payments were low value and so I don't think Nationwide needed to intervene. But by the time she made the third payment, even though she was paying an account in her own name, this was the third payment she'd made that day to a new payee. In the months prior to the scam the account was mainly used for low-value payments and so I agree £6,420 was out of character and represented an increase to the normal spending on the account. So, I think Nationwide missed an opportunity to intervene.

Nationwide should have contacted Mrs H and asked her some questions about the purpose of the payments and as there's no evidence she'd been told to lie, I think she'd have told it that she planned to make payments in cryptocurrency to a recovery agent. And, with further probing questions I think she'd also have disclosed that she had been cold called and that she'd also been told to download AnyDesk to her device.

This would have been enough information for Nationwide to have identified that she was being scammed and so it should have provided her with a tailored scam warning and advised her that there were red flags present. It should also have discussed with her the possibility that B was a clone of the genuine company and advised her to contact the details on the FCA website to check whether she was dealing with the genuine company.

Had it done this I'm satisfied the scam would have come to light and Mrs H wouldn't have made any further payments. Because of this I'm satisfied that Nationwide failed to intervene in circumstances which could have prevented her loss.

In reaching this conclusion I've considered the points Nationwide raised in response to our investigator's view. Firstly, it has said that there was a break in the chain of causation, so the onus was on W to intervene because the funds were lost from there to the scammer's account, while the transfers from Nationwide to W didn't give rise to Mrs H's loss. I accept the money wasn't lost directly from Mrs H's Nationwide account, but I'm satisfied that if it had identified that the spending was unusual for the account, it could have prevented her loss. So, even though the payment journey meant there was a later opportunity for another business to have done the same thing, this doesn't mean Nationwide didn't need to protect Mrs H when she made the payments.

Nationwide has also said there's a distinction between me-to-me scam cases involving payments to a regulated business and those involving payments to cryptocurrency exchange companies, namely that, in the former, there's no visibility that the transaction involves cryptocurrency and that there is a risk of an onwards payment. I accept the fact Mrs H was

paying her own account meant the nature of the payment alone wasn't enough to identify she might be at risk, but Nationwide is required to stop payments which are suspicious or unusual to protect customers who might be at risk of fraud, and the fact Mrs H wasn't paying a cryptocurrency merchant doesn't excuse it for having failed to do that.

Finally, Nationwide has suggested it would be entitled to seek a full contribution from W if this matter had been decided in a court. But this decision is based on what is fair and reasonable in all the circumstances of the complaint, which may be different to what a court would decide.

Contributory negligence

I accept there's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence but, in the circumstances, I don't think Mrs H was to blame for the fact she didn't foresee the risk. This is because she was dealing with a clone of a genuine company and so even though she did reasonable checks, it wouldn't have revealed the scam.

Mrs H had invested in cryptocurrency previously, so it wasn't unreasonable that she believed what she was told by the scammers. She also thought the request for a payment of tax was reasonable. So, I don't think she can fairly be held responsible for her own loss.

My final decision

My final decision is that Nationwide Building Society should:

- Refund £6420.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If Nationwide Building Society deducts tax in relation to the interest element of this award it should provide Mrs H with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs H to accept or reject my decision before 1 January 2024.

Carolyn Bonnell
Ombudsman