DRN-3269471

The complaint

Ms H complains that Tesco Personal Finance PLC ("Tesco") refuses to refund money she lost as part of a scam.

What happened

Ms H received a cold call from a merchant I'll refer to as 'A'. The caller explained that he worked as an adviser for A and could help her make a lot of money if she decided to trade with them. Ms H explained she was unemployed and was trying to save the money she had. But the adviser persuaded her that it would be better to invest than allowing her money to sit and earn little interest. The adviser explained he would show Ms H how to trade and she would be able to withdraw her money whenever she wanted.

Believing the adviser was genuine, Ms H agreed to open a trading account with A by depositing a small amount to start with. The adviser helped Ms A do this by remotely accessing her computer. Rather than paying A directly, Ms H was instructed to first purchase crypto with a company called 'X' and then load the crypto onto her wallet with A. Ms A initially made payments via another banking provider but was soon persuaded to add more money using her Tesco Mastercard credit card (which she'd recently opened). Ms H was shown significant profits and she agreed to deposit further larger amounts using a credit card account with another banking provider.

Ms H disputes four payments she made to X using her Tesco credit card totalling £3,193 (plus transaction fees of £127.41). All the payments were made on 25 September 2019. Ms H realised she'd been the victim of a scam when she was unable to withdraw her funds from her wallet with A and reported what had happened to Tesco.

Tesco concluded Ms H had no chargeback options or section 75 rights because she didn't pay A directly and instead purchased crypto via a legitimate crypto dealer (X). Unhappy with Tesco's response, Ms H referred her complaint to this service.

One of our investigators concluded A had scammed Ms H. She also concluded that Tesco failed to give Ms H a meaningful warning when she called it to unblock a payment to X. Our investigator felt it would be fair for Tesco to refund Ms H's losses. Ms H agreed with the outcome but Tesco didn't. It said in summary that:

- The conclusions were reached with a huge benefit of hindsight, leading to an unfair outcome.
- There is no evidence to support that A or X were known to be involved in scams as there are no regulator warnings about either of them.
- Ms H was transacting with a legitimate and genuine crypto currency convertor, one she had used before and was very much wanting the payments to go through. Based on this conversation, it had no concerns.
- It has a duty to carry out customers instructions and by doing otherwise it would be failing to meet its basic and fundamental obligations as a credit card provider.

- Most transactions to crypto currency converters are not later raised as scams and it is unfair to say Tesco should have acted differently in 2019 based on what was learned afterwards.
- The BSI code is not regulatory and doesn't obligate firms to warn customers of every potential scam. It is not regulated to give financial advice and the decision to go ahead with a purchase lies with the consumer.
- There was no indications that Ms H had fallen victim to a scam and even if it did say that scams exist in the crypto currency industry, this wouldn't have deterred Ms H from investing and had no concerns over making the payments.

The complaint has therefore been passed to me for determination.

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.

It isn't in dispute that Ms H has lost the money she invested. But the question I must consider here is the extent to which Tesco can be considered liable for her loss. I must also consider whether Tesco did all that it could have done when Ms H reported that she had been defrauded. In this particular case, I agree with our investigator that Tesco should refund her the amount she lost.

Tesco questions whether this was indeed a scam as there is no FCA warning about A or X. I've seen that the FCA first published a note titled 'About the FCA Warning List' in August 2017. Underneath the title headed 'If the firm isn't on the Warning List', it said 'Even if a firm isn't on the Warning List, it might still be a scam'.

So whilst I can agree with Tesco that an FCA warning or another regulator warning about a merchant does hold significant weight in indicating a scam. The FCA itself has concluded the absence of a warning doesn't mean a firm isn't a scam.

Because of this, it's helpful to understand what credible sources say about cryptocurrency scams and how this compares to Ms H's experience.

The City of London police published a note on cryptocurrency scams in August 2018. It said amongst other things:

> *'Fraudsters are cold calling victims and using social media platforms to advertise 'get rich quick' investments in mining and trading in cryptocurrencies. Fraudsters will convince victims to sign up to cryptocurrency investment websites and to part with their personal details such as credit card details and driving licences to open a trading account. The victim will then make an initial minimum deposit, after which the fraudster will call them to persuade them to invest again in order to achieve a greater profit.*
>
> *In some cases, victims have realised that they have been defrauded, but only after the website has been deactivated and the suspects can no longer be contacted.'*

The FCA also published a note titled 'Cryptoasset investment scams' in June 2018 where it noted:

> *'Scam firms can manipulate software to distort prices and investment returns…. They are also known to suddenly close consumers' online accounts and refuse to transfer the funds to them or ask for more money before the funds can be transferred.'*

I've found Ms H's testimony to be persuasive and it's entirely consistent with the description of cryptocurrency scams by the credible sources I've referenced. For example, she was cold called, promised large gains with the ability to easily access her funds. She invested with a smaller amount to start with and was encouraged to pay more after seeing significant gains through 'successful campaigns' within a short space of time. And Ms H has provided proof of this in the form of screenshots of her trading account with A. When she tried to withdraw her funds (as she believed she could), she was met with silence and A has since disappeared and is no longer in operation.

Ms H has also provided significant negative online customer reviews relating to A. Whilst this is circumstantial and not by itself 'proof' of fraud, it does add weight to the overall picture that A was operating a scam as described by the FCA and the police above. So, I am satisfied based on all I've seen that A scammed Ms H.

As I'm satisfied that Ms H was scammed, I'll now consider whether I think Tesco could have done anything to prevent it.

It is common ground that Ms H authorised the payments she made in 2019, even though she was duped into making them by A as part of a sophisticated scam. She used her security credentials to make the payments online and, in broad terms, the starting position in law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the terms and conditions of the customer's account. And under the Payment Service Regulations 2017, Ms H is presumed liable for the loss in the first instance.

However, taking into account the law, regulatory rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Tesco should fairly and reasonably:

- Have been monitoring accounts—and any payments made or received—to counter various risks, including anti-money-laundering, countering the financing of terrorism, and preventing fraud and scams;
- Have had systems in place to look out for unusual transactions or other signs that might indicate its customers were at risk of fraud (amongst other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer; and
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

In the context of this scam, Ms H paid funds from her Tesco credit card account to a cryptocurrency exchange, which she did with the assistance of A's adviser who guided her over the phone and through remotely accessing her computer. The crypto was immediately moved onto her wallet with A with the adviser's assistance. In this case, Ms H's initial two payments to X failed, the third was declined by Tesco due to it being a 'high risk' transaction. A fourth transaction attempt was processed successfully, though Tesco blocked Ms H's credit card immediately after the payment was made. Ms H called Tesco to unblock the credit card on 25 September 2019 in order to make a payment to X.

Tesco hasn't explained why it blocked the payments to X other than seeking to confirm the payments were genuine. But it had noted one of the payments as a 'high risk' transaction. I think given Tesco's clear concerns about payments being made to X (for whatever reason) it

should have had a conversation with Ms H before processing any of them. I consider it was appropriate for Tesco to have taken a close look at the payment before processing it.

The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018. And by January 2019, cryptocurrency scams continued to increase in frequency. So, by the time Ms H started making her investments using her Tesco credit card in September 2019, I think Tesco ought reasonably to have had a good enough understanding of how cryptocurrency scams work – including the fact that many consumers would first purchase crypto with a legitimate merchant before moving it on again to the fraudster.

Therefore, I'm satisfied that Tesco should've had mechanisms in place to detect and prevent this type of fraud at the time Ms H was making her payments. In my view, Tesco did have such mechanisms and did indeed intervene in order to ask Ms H further questions about the payment to X on 25 September 2019. Tesco said it sent a text message to Ms H asking her to confirm the payments were genuine. It placed a security block on her account and only after Ms H spoke with it was the block removed.

I've listened to the call and Tesco asked Ms H what transaction she was trying to do. Ms H talked through her attempted payments and continuously referred to 'we' when describing the payments she was trying to make. This ought to have been a concern. Tesco noted in the call that earlier payment attempts to X were blocked which Ms H acknowledged.

Whilst the adviser looked into the payment for several minutes, he came back and the following interaction happened:

> *Adviser: 'Can I just check what is it this company does?'*
>
> *Ms H: 'I've used it before'.*
>
> *Adviser: 'What is it this company do?'*
>
> *Ms H: 'Well it's like Bitcoins….and then I buy the Bitcoin and pay somebody else…it's hard to explain really'*
>
> *Adviser: 'Are you comfortable with that company having your details'*
>
> *Ms H: 'Errm, yeah well they've just got my email address mainly, as I said I've used them before and there was no problem'*
>
> *Adviser: 'I assume you just found this company online'*
>
> *Ms H: 'No I'm working with somebody who is helping me, as I've said I used them before and there was no problem last time'*

The adviser went onto explain that the type of transaction Ms H was making wouldn't be covered by chargeback dispute rights if something were to go wrong and Ms H accepted this.

I think Ms H volunteered information that ought to have been 'red flags' to Tesco. She referenced 'we' many times when discussing her payment attempts, explained someone was helping her and that she was purchasing Bitcoin and paying somebody else. Unfortunately (and not as Tesco suggest is with the benefit of hindsight) the caller did not appear to pick up on the warning signs.

Whilst Tesco asked Ms H if she was comfortable with the company having her details and explained chargeback rights wouldn't be available to her. It didn't actually warn about common cryptocurrency scams that on the face of it appeared like Ms H was falling victim to. I appreciate Ms H explained she'd dealt with the company before a number of times. But I don't think Tesco gave her reason to question why she would be sending her crypto to 'somebody else'.

Based on the answers Ms H gave during the phone call of 25 September 2019, I think Tesco ought to have had concerns that Ms H was at risk of falling victim to a scam. I think it could've reasonably done more to prevent Ms H from making the payments to the scammers. I don't think Tesco needed to probe any further based on the information provided by Ms H to have given her a meaningful warning about common cryptocurrency scams. It could have explained the risks of not having control of your own wallet, being coached by someone else and that many scam companies use legitimate looking websites with fake software to make it seem like your earning large profits to encourage further deposits. Tesco could have also explained its own customer experiences that the same firms would often block customers from withdrawing their funds. To be clear, I don't think Tesco ought to have provided Ms H with financial advice but the FCA and its predecessor explained has already explained that a scam warning wouldn't constitute financial advice. So in these circumstances, I consider it would be fair and reasonable to hold Tesco liable for failing to provide Ms H with a meaningful scam warning when it had grounds to do so.

I think a more meaningful warning would have stopped Ms H in her tracks, even though she had used A before, because the warning would have been reflective of her experiences with A. And whilst she hadn't yet attempted to withdraw her funds, I think she would have likely tried to before paying them anymore money.

Ms H believed that A was legitimate and her account manager gained her trust by explaining he would coach her through her investments. She had access to an online wallet and saw her investments performing. I don't think she could have reasonably known about the operation of this type of scam unless prompted by for instance, a financial professional like Tesco. I think the onus was on Tesco to inform Ms H of the risk that she would likely lose all of her money if she sent her cryptocurrency to somebody else.

Whilst the transaction fees were not paid to X directly and were instead charged by Tesco for Ms H using her card to pay X, I do not think these would have been incurred had Tesco provided a meaningful warning to Ms H. So these payments should also be refunded.

My final decision

My final decision is that I uphold this complaint and require Tesco Personal Finance PLC to:

- Refund all Ms H's payments to X, this should include any associated transaction fees;
- Refund interest and charges applied to Ms H's Tesco credit card in respect of the payments to X.
- Pay 8% interest on any payments Ms H's made towards her Tesco credit card in relation to the payments to X. If Tesco deducts tax in relation to the interest element of this award, it should provide Ms H with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms H to accept or reject my decision before 8 April 2022.

Dolores Njemanze
Ombudsman