DRN-4969377

The complaint

Miss T complains that HSBC UK Bank Plc trading as first direct ('first direct') won't reimburse the money she lost when she fell victim to a scam.

What happened

Miss T is represented in this case but for ease I'll refer to Miss T throughout my decision.

Miss T says that an acquaintance of hers posted something on a social media platform about a cryptocurrency investment coach I'll refer to as C. She didn't know at the time, but her friend's account had been hacked. Miss T followed C and then received a direct message from her. C claimed to be a professional bitcoin miner who wanted to pass on information about mining and provide step by step guidance to help her to trade. The messages referred to huge daily profits and a 10% rate of commission.

Miss T asked for additional information and C told her that the minimum investment was £500, and the profit would be £10,150. C said she would send Miss T details of the broker's website and that she would need to register and then she could see the profit she had earned.

Miss T made three payments from her first direct account. The first two were both debit card payments of £1,029.90 to a known cryptocurrency exchange. These transactions were authorised on 15 August 2023 but appear on Miss T's statement after this. The third transaction was a faster payment of £3,300 to a named individual on 16 August 2023.

Miss T realised she was the victim of a scam when she was asked to send more funds. She reported what had happened to first direct, which investigated the card payments and faster payment separately. In respect of the card payments, first direct said that as Miss T had paid an account in her own name at a cryptocurrency exchange it couldn't raise a dispute. First direct considered the faster payment under the Lending Standards Board's Contingent Reimbursement Model Code (CRM Code) and said that both it and the receiving bank had sufficient fraud prevention measures in place. But first direct said Miss T should have taken more care and completed more checks before the transaction was made.

Miss T was unhappy with first direct's response and brought a complaint to this service.

Our investigation so far

The investigator who considered this complaint didn't recommend that it be upheld. He said the CRM Code applied to the faster payment and first direct provided an effective warning in respect of it. The two card payments of £1,029.90 each weren't covered by the CRM Code and weren't so unusual that first direct ought reasonably to have intervened.

Miss T didn't agree with the investigator's findings. She said that over a 24 hour period she made payments totalling over £5,000 to a cryptocurrency exchange and first direct should have considered this to be unusual. She referred to FCA and Action Fraud warnings about cryptocurrency scams from 2018. Miss T also said that aside from a payment for a medical procedure, she hadn't made high value transactions in the twelve month period before the scam.

The complaint was passed to me to decide. I was minded to reach a different outcome to the investigator and require first direct to reimburse 50% of the faster payment (after taking into

account an amount that could have been recovered) plus interest. I issued a provisional decision on 17 July 2024 and said in the "What I have provisionally decided – and why" section of it:

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 take into account 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.

In broad terms, the starting position in law is that first direct is expected to process payments that a customer authorises it to make, in accordance with the terms and conditions of the customer's account and the Payment Services Regulations (PSR's).

The CRM Code, which first direct has signed up to, doesn't apply to the card payments Miss T made. This is because it doesn't apply to card payments or international payments. But I've gone on to consider first direct's wider obligations to look out for out of character transactions or other signs that its customer might be at risk of fraud. This is the case irrespective of the payment channel used.

I accept that the card payments were going to a known cryptocurrency exchange and that this service considers that from January 2023 firms ought to have recognised the increased risk associated with cryptocurrency related payments. But I'm not persuaded that first direct needed to do anything more in respect of them given their value (the total value of the two transactions was just over £2,000), and the fact that an unusual pattern of payments hadn't emerged.

Miss T's representative has said that the card payments followed the faster payment, but this is incorrect. I have noted above that the two card payments were authorised on 15 August 2023. Also, Miss T didn't make payments of over £5,000 to a cryptocurrency exchange in a short period of time as her representative has advised. The faster payment was to a named individual.

I turn now to the faster payment of £3,300 which is covered by the CRM Code. The CRM Code requires firms to reimburse victims of APP scams like this one unless it can establish that it can rely on one of the following exceptions to reimbursement:

- The customer made payments without having 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' by failing to take appropriate steps in response to that warning.

There are further exceptions outlined in the CRM Code that do not apply to this case.

Miss T's representative has suggested that she was vulnerable at the time of the scam because she began investing in the early hours of the morning and hadn't slept for around forty hours.

If Miss T was vulnerable as set out in the CRM Code, she would be entitled to full reimbursement without considering the exceptions I have listed above.

Whilst a lack of sleep will have had an impact, I'm not persuaded it rendered Miss T unable to protect herself from the scam she fell victim to. She has said that she read social media testimonials before deciding to invest, and there's no indication she was under pressure to act immediately.

Did Miss T have a reasonable basis for belief?

Taking into account all of the circumstances of this case, including the characteristics of Miss T and the complexity of the scam, I think first direct can fairly rely on an exception to reimbursement set out in the CRM Code. I'm not satisfied that she had a reasonable basis for believing the payment was for a genuine investment opportunity. Whilst I recognise Miss T first heard about the investment through a friend (although the friend's account had been hacked) I don't consider this meant she should have accepted everything at face value, particularly given the following points:

- Genuine investments aren't arranged over social media.
- C said she worked with a certain platform Miss T was given a link to. I can't see a genuine company with that name or any reviews, which I consider ought reasonably to have concerned Miss T.
- The rate of return offered was unrealistic and too good to be true. Miss T was told that if she invested a minimum amount of £500, she would get £10,150. The messages also refer to short timescales to receive huge profits.
- An early message from C said that "*your profit is always 100%*" so it seems that profits were guaranteed. I consider this was a serious red flag that something wasn't right.
- Miss T didn't receive a contract or any other documentation to set out the terms of her agreement with C.
- The faster payment to an individual is the final transaction Miss T made. Miss T says the payment was an additional commission fee after she had been asked to pay a fee for withdrawing. The reason given for each payment became less plausible and there is no indication Miss T was advised that any fees would be due when she first chose to invest. Miss T has referred to checking additional payments with her friend (whose account had been hacked), but the messages I have been provided with relate to a payment of £500 for a further upgrade so don't seem to be relevant here.

The CRM Code also sets out standards that firms are required to meet. Where these are not met, the firm may still be liable to reimburse a victim in part, even where it has been able to establish that an exception to full reimbursement can be fairly applied (as is the case here). Those requirements include the provision of what the CRM Code defines as an "Effective Warning" when a firm identifies an APP scam risk in relation to a payment. In order for a warning to be 'Effective' under the CRM Code. It must, as a minimum be: clear, specific, understandable, timely and impactful.

The CRM Code requires that warnings be both specific to the scam risk identified and impactful – to positively affect a customer's decision-making in such a way that the likelihood of an APP scam succeeding is reduced. The CRM Code goes on to say this should include steps to ensure that the customer can reasonably understand the consequences of continuing with an irrevocable payment.

I consider that first direct should have provided Miss T with an effective warning when she made the faster payment. It was a higher value transaction and followed card payments to a cryptocurrency exchange. But I don't agree that first direct ought reasonably to have spoken to Miss T and asked probing questions as she has asserted. This level of interaction would cause too much disruption to many legitimate low value transactions.

I've considered the warning that was provided and don't agree with the investigator that it was effective. When she made the payment Miss T said it was for an investment and was provided with a warning tailored to investment scams. I asked Miss T what she thought about the warning, and she explained that she found the screens to be of little help to her.

The warning is lengthy, so I won't set it out in full here. It starts with a warning that if someone has told a customer to mislead first direct or give the wrong payment reason this is

a scam. This wording didn't apply to Miss T. There is then a list of things a customer needs to do before making the payment. The warning tries to cover off too much information to have any real impact and fails to bring to life some of the key features of the scam Miss T fell victim to. For example, there is no mention of investments advertised on social media. Overall, I'm not persuaded the warning was effective as set out in the CRM Code.

As I have reached the conclusion that the warning first direct provided wasn't effective, it's also clear that Miss T didn't ignore an effective warning so first direct can't reasonably rely on this exclusion to reimbursement either.

Under the CRM Code, first direct should reimburse Miss T 50% of the faster payment.

I have considered whether first direct did enough to recover Miss T's funds when she reported the scam. I have seen evidence which confirms that Miss T reported the scam within an hour and a half of the faster payment being made. Evidence I have seen from the bank that received Miss T's funds shows that £3,270 was removed from the account within minutes of crediting it. A further transaction for £28 was made many hours later. I have not been provided with any information about the remaining £2. In the circumstances, I consider HSBC should reimburse £30 (and then pay Miss T 50% of £3,270).

Responses to my provisional decision

Miss T accepted my provisional findings. First direct didn't. It said several points in its warning were relevant to Miss T, but she chose to invest without getting independent financial advice, without checking the FCA register or checking whether the person she was communicating with was a genuine representative of the company. Given that I have reached the conclusion that Miss T didn't have a reasonable basis for believing the investment opportunity was genuine, first direct said it was unfair to hold it liable.

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, my final decision is the same as my provisional decision (reproduced above) and for the same reasons.

For the reasons set out in my provisional decision, I'm not satisfied that the warning first direct provided when Miss T made the faster payment was effective, so, under the provisions of the CRM Code, she should be reimbursed 50% of her loss (after taking into account recovered funds or funds that could have been recovered – as discussed in my provisional decision). Whilst parts of first direct's warning could apply to Miss T, the warning lacks impact and doesn't mention social media investments or bring investment scams of this nature to life.

Putting things right

Overall, I'm satisfied that first direct should reimburse Miss T in the manner set out in my provisional decision and below.

My final decision

I uphold this complaint and require HSBC Bank Plc trading as first direct to:

- Pay Miss T £30 that could have been recovered; and
- Pay Miss T £1,635, and
- Pay interest on the above amounts at the rate of 8% simple per year from the date of

loss to the date of settlement.

If HSBC Bank Plc trading as first direct considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Miss T how much it has taken off. It should also give Miss T a tax deduction certificate if she asks for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss T to accept or reject my decision before 12 September 2024.

Jay Hadfield
Ombudsman