DRN-4567012

The complaint

Mr H complains that Lloyds Bank PLC won't reimburse him the money he transferred to a fraudster.

What happened

Mr H has explained he was looking for a 'work from home' position and had applied for roles on a known employment website. He received communication from an individual via an instant messaging app offering a freelance position where, to simplify, Mr H would be required to 'click' online product data which would essentially generate star-rating reviews for that product, boosting its position in the market. Mr H was told that by doing this, he could earn around £1,000 a week, but in order to complete the role, as the company was 'expanding internationally through advanced technology', Mr H would be required for 'security purposes' to have an encrypted wallet.

Mr H has said he searched for the company online and found details on Companies House, which reassured him that the company was genuine. However, unbeknownst to Mr H at the time, he was in fact dealing with a fraudster, impersonating a genuine firm of the same name.

The fraudster talked Mr H through setting up a cryptocurrency account and further details of the role, as well as setting him up an account on their website. Mr H has explained that the individual he was speaking with gained his trust by initially appearing to use their own money to help withdraw Mr H's first 'commission'.

Mr H was then told that to withdraw further commissions and bonuses, he would need to first make a deposit, which he would then get back. He's explained he was threatened and pressured into doing so, being told that if he didn't make the withdrawal, the merchant wouldn't wait, and he would lose everything. On this basis, in January 2023, Mr H made a payment of £316 to an individual's personal account.

When the fraudster continued to ask for further deposits and Mr H was unable to withdraw his money, he began looking online again and identified that others had been tricked by this same scam. Mr H contacted Lloyds via instant messaging in April 2023 and was advised to call its fraud line. However Mr H has explained that as he was busy with work, he didn't contact Lloyds until June 2023, at which point his fraud claim was investigated.

Lloyds investigated Mr H's fraud claim and considered its obligations to provide Mr H with a refund. Lloyds considered Mr H's complaint against the Lending Standards Board Contingent Reimbursement Model (CRM) Code, which it is a signatory of. The CRM Code requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. Lloyds says one or more of those exceptions applies in this case.

Lloyds has said Mr H didn't have a reasonable basis for believing he was making a genuine payment. Lloyds considers Mr H ought to have done more checks to make sure the person he was making the payment to was genuine.

It also contacted the beneficiary bank to attempt to recover Mr H's money, but unfortunately no funds remained in the account.

Mr H disagreed with Lloyds so brought the complaint to our service. One of our investigators considered the case and didn't uphold it – he thought it was more likely than not that the CRM Code didn't apply in this case, but if so in any event, thought Mr H ought to have completed further checks to verify that he was dealing with a genuine company. If the CRM Code wasn't to apply, the investigator considered the payment wasn't sufficiently out of character that Lloyds ought to have intervened before processing the payment. The investigator therefore didn't consider that Lloyds needed to do anything to put things right for Mr H.

Mr H didn't agree with the investigator, so the case has been referred to me for a decision.

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, while I'm sorry to disappoint Mr H, I'm not upholding his complaint. I'll explain why.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. However, where the consumer made the payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the consumer even though they authorised the payment.

When thinking about what is fair and reasonable in this case, I've considered whether the CRM Code applies to Mr H's claim and if so, whether Lloyds should have reimbursed Mr H under its provisions - and whether it ought to have done more to protect Mr H from the possibility of financial harm from fraud. As it's not clear whether Mr H's claim is covered by the Code, I've also considered whether there are any other provisions under which Mr H should have been reimbursed by Lloyds.

The CRM Code

As I've mentioned, Lloyds is a signatory of the Lending Standards Board Contingent Reimbursement Model (CRM) Code. The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams, in all but a limited number of circumstances and it is for Lloyds to establish that a customer failed to meet one of the listed exceptions set out in the CRM Code.

However, the CRM Code doesn't apply to all authorised push payments – for example, it doesn't cover purchases from a third party on a cryptocurrency exchange site that are then sent on to a fraudster. They also don't cover faster payments to international accounts. In this case, it's not entirely clear what the nature of Mr H's payment transfer was – there was clearly an element of the scam that involved cryptocurrency, in order for the fraudster to have asked Mr H to set up a cryptocurrency account – but it's not entirely clear how this account came into play in this scam. This is particularly the case here as from the statements I've seen, the cryptocurrency account doesn't show any previous activity.

It's also not entirely clear what the final destination of Mr H's funds was – his funds were initially sent to an intermediary payment service provider, so from here it's also possible they entered a cryptocurrency wallet, or an international account, neither of which the CRM Code covers.

If I assume the payment Mr H made *is* covered by the Code, a bank may choose not to reimburse a customer if it can establish that*:

- The customer ignored what the CRM Code refers to as an "Effective Warning" by failing to take appropriate action in response to such an effective warning
- 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

**Further exceptions outlined in the CRM Code do not apply to this case.*

I think Lloyds has been able to establish that it may choose not to fully reimburse Mr H under the terms of the CRM Code. I'm persuaded one of the listed exceptions to reimbursement under the provisions of the CRM Code applies.

Taking into account all of the circumstances of this case, including the characteristics of the customer and the complexity of the scam, I think the concerns Lloyds has raised about the legitimacy of the transaction Mr H was making are enough to support its position that he didn't have a reasonable basis for believing he was paying a legitimate employer. I'll explain why.

First, I think it's important to consider that the Code is set up to cover scam payments intended for genuine or legitimate purposes. In this case, Mr H has explained that he understood his employment to be, in essence, creating falsified ratings on online products. I think this in itself is an indication that Mr H's claim ought not to be covered by the Code, as the nature of the work doesn't appear to be a legitimate service for a firm to offer.

In any event, I think there were enough other red flags here that Mr H ought reasonably to have taken caution before proceeding to make payment. I appreciate that Mr H had looked up the legitimate firm that the fraudster was falsifying, which gave him reassurance that this was a genuine role. However, having looked at the genuine firm's website, I can see that they are involved in 'property data' – which doesn't correspond with the tasks Mr H was being asked to complete.

The fraudster provided Mr H with an explanation of how the role worked, and why he needed to open a cryptocurrency wallet. While the fraudster used a lot of technical terms and jargon, I don't consider they ever gave a particularly plausible reason why a cryptocurrency account was required. I also don't think it's realistic that a firm would require its staff to provide a deposit to access commission payments owed – only for the firm to then reimburse that same deposit.

Mr H was told that by completing the work, he could earn around £1,000 a week. I think this level of salary ought to have raised concerns, based on the apparent simplicity of the task and lack of any skills required – it seems too good to be true for the level of output required.

Mr H has said he was threatened and pressured to make the deposit and given time restrictions to do so – again I don't think this is how a legitimate firm would be expected to behave, particularly when the payment the worker is attempting to withdraw is something already earned. It's also unclear why he would need to pay an account in an individual's name, rather than the business' own account if it was a legitimate deposit he was making.

With all of the above in mind, in the particular circumstances of this case, I consider that Mr H ought to have had concerns about the payment he was making and that, in turn, ought to have led to a greater degree of checking on Mr H's part. In not carrying out sufficient checks I don't find he had a reasonable basis for believing he was making a genuine payment and so fell below the level of care expected of him under the CRM Code.

Should Lloyds have done more to try to prevent the scam and protect Mr H?

I've thought about whether Lloyds did enough to protect Mr H from financial harm.

The CRM Code says that where firms identify APP scam risks in a payment journey, they should provide Effective Warnings to their customers. The Code also says that the assessment of whether a firm has met a standard or not should involve consideration of whether compliance with that standard would have had a material effect on preventing the scam.

I am also mindful that when Mr H made this payment, regardless of whether the payment is covered by the Code or not, Lloyds should fairly and reasonably also have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things).

Having considered the payment Mr H made, I don't think it was so remarkable, in comparison to his usual account activity, that it should've appeared as suspicious to Lloyds. I therefore don't think Lloyds failed to meet its standards under the Code by not providing Mr H with an effective warning, prior to processing the payment, or that outside of the Code, Lloyds should have intervened further before processing the payment.

Once it was made aware of the scam, Lloyds tried to recover Mr H's funds the same day, but unfortunately was advised that no funds remained. I don't think Lloyds could reasonably have done anything further to recover Mr H's payment, particularly due to the time that had already passed since the scam had taken place.

Overall, I'm satisfied that Lloyds' position on Mr H's fraud claim is fair and reasonable in all of the circumstances and that Lloyds shouldn't be held liable for Mr H's losses. And so I don't intend to make an award to Mr H.

My final decision

My final decision is that I don't uphold Mr H's complaint against Lloyds Bank PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 6 March 2024.

Kirsty Upton
Ombudsman