

THE COMPLAINT

Mr L complains that HSBC UK Bank Plc (trading as First Direct) will not reimburse him money he says he lost when he fell victim to a fraud.

WHAT HAPPENED

The circumstances of this complaint are well known to all parties concerned, so I will not repeat them again here in detail. However, I will provide an overview.

Mr L's First Direct debit card was used to make three transactions ("the Transactions") on 5 December 2024 at a place I will refer to as 'Establishment A' in this decision. The Transactions were for £4989.56, £980 and £4,9831.81. Mr L says he did not consent to the Transactions. He also says he did not consent to a transfer made from his savings account to his current account at the same time.

Mr L disputed the above with First Direct. When First Direct refused to reimburse Mr L, he raised a complaint, which he also referred to our Service.

One of our investigators considered the complaint twice, and did not uphold it on both occasions. As Mr L did not accept the investigator's findings, this matter has been passed to me to make a decision.

WHAT I HAVE 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 find that the investigator at first instance was right to reach the conclusion he did. This is for reasons I set out in this decision.

I would like to say at the outset that I have summarised this complaint in far less detail than the parties involved. I want to stress that no discourtesy is intended by this. If there is a submission I have not addressed, it is not because I have ignored the point. It is simply because my findings focus on what I consider to be the central issues in this complaint.

Further, under section 225 of the Financial Services and Markets Act 2000, I am required to resolve complaints quickly and with minimum formality.

Key findings

Under the Payment Services Regulations 2017, there are two things that need to be satisfied for a payment(s) to be considered authorised. They are authentication and consent. Turning to authentication. Based on the technical evidence before me, I am persuaded that the Transactions were authenticated. I deal with consent below.

Mr L's physical debit card and PIN code were used to make the Transactions. Below are three possible scenarios in this case:

- (a) Mr L consented to the Transactions by making them himself using his card and PIN.
- (b) Mr L consented to the Transactions by providing his card and PIN to a third-party so they could make the Transactions.
- (c) A third-party obtained Mr L's card and PIN and made the Transactions without Mr L's consent.

In scenarios (a) and (b), Mr L would not be entitled to redress. In scenario (c), Mr L could potentially be entitled to redress. Mr L disputes scenarios (a) and (b). Therefore, I have considered whether, on the balance of probabilities, scenario (c) applies.

For scenario (c) to apply, a third-party would have needed to be in possession of Mr L's physical card. Mr L says that he put his card behind the bar at Establishment A. This provides some explanation as to how a third-party may have come into possession of Mr L's card. However, this does not explain how the third-party obtained Mr L's PIN, which would have been required to make the Transactions. Mr L says he did not share his PIN with anyone.

Mr L's PIN could have been viewed in the First Direct banking app on Mr L's mobile phone. Mr L says that his phone was also behind the bar at Establishment A. I have thought about whether a third-party may have accessed Mr L's phone and viewed his PIN code. Having done so, I am not persuaded this could have happened. I say this because First Direct's technical evidence does not support this proposition. That is, it does not show that Mr L's PIN was viewed in his banking app on his phone during the time concerned.

Mr L says that the taxi driver that drove him to Establishment A may have seen him entering his PIN code when withdrawing money from an ATM. I attach little weight to this as Mr L has provided little to support this proposition. In fact, Mr L has stated he cannot remember if the taxi driver was nearby at the time of the cash withdrawal.

Mr L has alluded to two other potential scenarios in terms of how his PIN may have been compromised.

First, Mr L says that his mobile phone was passcode protected. He says that the first two digits of his passcode at the time were 00, and the remaining four digits were the same as his First Direct debit card PIN. The suggestion is that a third-party 'shoulder surfed' Mr L when he entered his passcode into his mobile phone, worked out that the last four digits of the passcode was Mr L's card PIN, and then the third-party made the Transactions.

Second, Mr L says that his cards with other banks were also compromised at Establishment A. Some of those cards, Mr L claims, had the same PIN code as his First Direct debit card. Mr L also says that one of the other banks, which I will refer to as Bank T, confirmed that his PIN was viewed in his Bank T banking app before the Transactions were made. The suggestion is that a third-party somehow managed to access Mr L's mobile phone, accessed Mr L's Bank T banking app, viewed the PIN, worked out that the PIN was the same for Mr L's First Direct card, and then made the Transactions.

I find these suggestions somewhat questionable and difficult to accept. I say this in particular because Mr L says that a transfer was made from his savings account to his current account which he did not do. For this to have happened, a third-party would have needed to know Mr L's First Direct banking app passcode, which Mr L says "*... the First Direct App can be accessed without biometric authentication by using a digital PIN. My phone login was similar to this but not exactly the same.*" This begs the question – how did a third-party work out the passcode to Mr L's First Direct banking app?

In any event, even if I were to accept third-party involvement in this case, I would find that Mr L acted with gross negligence.

Regulation 72 of the Payment Services Regulations 2017 states:

(1) A payment service user [in this case, Mr L] to whom a payment instrument has been issued must—

(a) use the payment instrument in accordance with the terms and conditions governing its issue and use

(3) The payment service user must take all reasonable steps to keep safe personalised security credentials relating to a payment instrument or an account information service.

Regulation 77 states:

(3) The payer is liable for all losses incurred in respect of an unauthorised payment transaction where the payer—

(a) has acted fraudulently; or

(b) has with intent or gross negligence failed to comply with regulation 72 (obligations of the payment service user in relation to payment instruments and personalised security credentials).

To be satisfied that an individual has acted with gross negligence, I would need to be satisfied that the individual showed a very significant degree of carelessness. When assessing this, I need to consider what a reasonable person would be expected to do in the circumstances concerned.

Mr L had never been to Establishment A before the date in question – describing it as “*not a 'high-end' establishment*”. Despite this, Mr L placed his debit card – and potentially other bank cards – and his mobile phone behind the bar because he was asked to do so regarding the former, and because he wanted to charge the latter. Even if Mr L did not appreciate the potential dangers of doing this, I would have expected him to have been aware of the dangers of, amongst other things, his card being used to make contactless payments. Further or alternatively, as Mr L has stated, some of his other bank cards had the same PIN code as his First Direct debit card.

For the above reasons, I think Mr L fell below what one would expect of a reasonable person in Mr L’s circumstances. Therefore, I find that Mr L acted with gross negligence, and not in accordance with Regulation 72(3).

I recognise that Mr L says he was intoxicated at the time in question. However, this is not something I can fairly hold First Direct accountable for.

First Direct intervened in the first Transaction by sending an SMS text message to Mr L’s mobile phone. This was responded to confirming the payment as genuine. I find that First Direct’s intervention was proportionate. I would not have expected First Direct to have intervened again given the response to the SMS text message.

Taking all the above points together, I find, on the balance of probabilities, that it is likely either scenario (a) or (b) (set out above) occurred in this matter. If it could be argued otherwise, I find that Mr L acted with gross negligence. My findings also apply to the transfer that Mr L says was made from his savings account to his current account.

Conclusion

I do not find that First Direct has done anything wrong in the circumstances of this complaint. Therefore, I will not be directing First Direct to do anything further.

In my judgment, this is a fair and reasonable outcome in the circumstances of this complaint.

MY FINAL DECISION

For the reasons set out above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr L to accept or reject my decision before 12 January 2026.

Tony Massiah
Ombudsman