DRN-6146091

THE COMPLAINT

Mr A complains that PayPal UK Ltd ("PayPal") will not reimburse him money he says he lost when he fell victim to fraud.

Mr A is represented in this matter.

WHAT HAPPENED

On 8 January 2026, I issued a provisional decision not upholding this complaint. I attach a copy of that provisional decision below – both for background information and to (if applicable) supplement my reasons in this final decision. I would invite the parties involved to re-read the provisional decision.

RESPONSES TO MY PROVISIONAL DECISION

Mr A's representative provided screenshots said to show Mr A owns his computer, along with information about the malware he says infected it and a recording of the alleged PayPal messages. The representative argues that because the malware enabled remote access control, PayPal would not have been able to detect this. They also say Mr A has colleagues in the cybersecurity industry who are willing to discuss the matter further.

I provided the above to PayPal and requested its comments.

In response, PayPal stated, in short, that Mr A's evidence did not, "… *conclusively prove unauthorised access … whilst we acknowledge the malware evidence provided, it does not demonstrate causation, such as remote sessions or compromise tied specifically to these transactions* … ."

PayPal also highlighted inconsistencies in the name and email address of Mr A's representative and noted that the representative's emails were written in the first person. PayPal suggested that Mr A may have written the emails himself and sent them under the representative's name.

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.

The evidence provided by Mr A's representative is circumstantial. While it indicates the possible presence of malware on his computer, the crucial link between that malware and the transactions in question is missing. I have not seen any persuasive evidence showing that the malware caused the transactions to be made. Although the malware may have been capable of this, that possibility alone does not demonstrate that it occurred. I have not seen anything compelling to support that proposition.

I do not consider it necessary for me to discuss this complaint with Mr A's colleagues. I also make no finding regarding PayPal's comments about Mr A's representative.

Taking all the above points together, I will not be departing from my provisional findings.

MY FINAL DECISION

For the reasons set out above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 11 March 2026.

COPY OF PROVISIONAL DECISION DATED 8 JANUARY 2026

I have considered the relevant information about this complaint.

The deadline for both parties to provide any further comments or evidence for me to consider is 22 January 2026. Unless the information changes my mind, my final decision is likely to be along the following lines.

If I do not hear from Mr A, or if he tells me he accepts my provisional decision, I may arrange for the complaint to be closed as resolved without a final decision.

THE COMPLAINT

Mr A complains that PayPal UK Ltd ("PayPal") will not reimburse him money he says he lost when he fell victim to fraud.

Mr A is represented in this matter. However, where appropriate, I will refer to Mr A solely in this decision for ease of reading.

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.

On 27 December 2024, three payment transactions were made from Mr A's PayPal account to another account not in his name. The payments were for the following amounts: $671.90, $359.95 and $659.90 USD. I will refer to these collectively as the "Transactions". Mr A says that he did not consent to the Transactions.

Mr A disputed the above with PayPal. When PayPal refused to reimburse Mr A, he raised a complaint.

One of our investigators considered the complaint and upheld it. She held that the Transactions were not authorised and so directed PayPal to reimburse Mr A the

Transactions in GBP equivalent, plus 8% simple interest. PayPal rejected this.

As PayPal did not accept the investigator's findings, this matter has been passed to me to make a decision.

WHAT I HAVE PROVISIONALLY 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 wrong to reach the conclusion she 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.

Issue(s)

The issue I must determine in this case is whether, on the balance of probabilities, a third-party made the Transactions without Mr A's consent.

If I conclude that Mr A did not consent to the Transactions, then he could potentially be entitled to a refund. On the other hand, if I conclude that Mr A consented to the Transactions – by making them himself or providing consent to a third-party to do so – then he will be liable for them and will not be entitled to a refund.

Mr A

Mr A has provided the following key material:

- Screenshots of, according to Mr A, "*Microsoft Defender Antivirus*" removing malware from Microsoft Windows. These removals are said to have taken place at or around the time the Transactions were made.

- Emails of what appears to be Google security alerts showing that: a Google account password had been changed, a Google Authenticator app was removed, a Google Authenticator app had been added, and a new device had been used to sign into a Google account.

- A letter dated 26 February 2025, from First Direct to Mr A stating, amongst other things, "*I confirm that on 27 December 2024, we sent you a text message regarding a Debit Card transaction attempt to the company Kraken Exchange. In line with our current policy, we held this payment for additional security checks and subsequently reversed it after you confirmed you had not actioned the payment*."

- SMS text messages purporting to be from PayPal alerting Mr A to the third and final Transaction.

Mr A's position, in short, is that he did not make the Transactions. He suggests that a third-party hacked his computer and made them: "*To provide some further information, it appears*

his [Mr A's] *computer was hacked and infected with a virus at the time of the fraudulent transactions*." Mr A relies on the material (set out above) to support this proposition.

PayPal

PayPal has provided the following key material showing:

- An IP address (the "IP Address") used to access Mr A's PayPal account from 1 September 2024 to 29 January 2025.
- A device (the "Device") used to access Mr A's PayPal account from 13 March 2012 to 26 January 2025.
- The IP Address and Device were used to access Mr A's PayPal account on 27 December 2024 at 13:24.
- The IP Address and Device were used to make the three Transactions on 27 December 2024 at 13:32, 13:38 and 13:57.
- On 27 December 2024, at 14:00, a different device was used to access Mr A's PayPal account. However, this device used the same IP Address.

PayPal's position, in short, is that the above suggests that Mr A consented to the Transactions.

My findings

Mr A's screenshots showing malware being removed, do not indicate which device they relate to. Without this link, I cannot conclude that the device Mr A says was compromised was the one used to make the Transactions.

Even if malware was on the Device shown in PayPal's evidence, I have not seen anything persuasive proving that the malware resulted in a full compromise. That is to say, the malware bypassed all the security measures Mr A had in place on his devices. Malware presence in and of itself does not necessarily mean an account takeover has taken place in the way Mr A is suggesting. Mr A says that all his devices had security protections. Therefore, I would expect to see further persuasive evidence that the malware he is relying on was able to bypass the security measures he had in place, which then allowed a third-party to make Transactions.

For the above reasons, I am unable to safely conclude that the Device was compromised.

It follows that the IP Address would be used to access Mr A's PayPal account and make the Transactions, which PayPal's evidence indicates. This is also supported by PayPal's argument: "*If* [Mr A's] *device was being accessed and controlled by a third-party, our security system would show a different or hidden IP address used on the account, although this is not the case*."

PayPal's evidence also shows that the IP Address and Device have been used consistently to access Mr A's PayPal account over a significant period. These were also used to make genuine payments before the Transactions. While the investigator noted that IP addresses can sometimes match, I have not seen any persuasive evidence to suggest that the IP Address Mr A has been using since 1 September 2024, was not the same one used to make the Transactions. This is supported by the fact that PayPal's evidence indicates the same Device, linked to Mr A's account since 13 March 2012, was also used to make the

Transactions.

Taking all the above points together, they suggest continuity, rather than compromise.

I acknowledge that there are some unexplained features of Mr A's case, such as the Google Authenticator security alerts, First Direct's letter and the SMS text messages purportedly from PayPal. However, to my mind, those points do not outweigh what I have set out above – particularly the fact that PayPal's evidence demonstrates continuity and a longstanding IP Address and Device being used.

In the absence of compelling evidence of account compromise/security bypass, I am not satisfied, on the balance of probabilities, that a third-party made the Transactions without Mr A's consent. It follows that PayPal is entitled – if it wishes – to pursue Mr A for any outstanding balance owed on his PayPal account.

Charities

I have listened to Mr A's telephone calls with our Service. Given the content of some of the calls, I would like to draw Mr A's attention to the below charities. It is entirely a matter for Mr A in terms of whether he wants to make contact with the charities.

- Papyrus (prevention of young suicide): www.papyrus-uk.org/ ; 0800 068 41 41
- StepChange (debt charity): https://www.stepchange.org/ ; 0800 138 111

MY PROVISIONAL DECISION

For the reasons set out above, I am currently minded not to uphold this complaint.

Tony Massiah
Ombudsman