DRN-5763862

The complaint

S, a limited company, complains that Barclays Bank UK Plc have declined to refund them for payments that they say weren't authorised. They'd like the funds returned to them.

S have appointed professional representatives for this case, but for ease of reading I'll only refer to S.

What happened

In April 2024 S were contacted by someone claiming to work for Barclays, saying there had been attempted fraud on their account. They were persuaded to download software which allowed the caller to remotely access their computer.

The caller then used this remote access to set up nine payments using the Barclays.net batch payment system. These were then authenticated using S' genuine smart cards and Sign What You See (SWYS) card reader. In total £64,261 left S' account, which they were not expecting. This included £763 to a pre-existing payee, which was returned. But S lost £63,498. The fraudster also attempted to make a transaction using S' online banking, but this was blocked by Barclays.

S reported these to Barclays, saying they hadn't agreed to them, and asked to be refunded. Barclays investigated and initially recovered £6,948.04. But they declined to offer a further refund. They said that the use of S' genuine payment tools meant they considered the payment correctly consented to and authorised. They also felt that they had provided sufficient warnings to S about scams. They did not see that S would be covered by the Lending Standards Board's Contingent Reimbursement Model (CRM).

Not happy with this answer S referred their complaint to our service. Further payments of One of our investigators looked at what happened, and he thought the complaint should succeed in part. He was satisfied that it was reasonable for Barclays to treat the payments as authorised. But he felt that Barclays systems had detected remote access before the authorisation and could reasonably have seen there was a risk. He thought it Barclays had declined the transactions until they had spoken to S the fraud would likely have come to light.

But he thought that S should bear some liability for the transactions as well – and suggested the remaining losses be split equally. He also thought Barclays should add 8% simple interest per annum for this amount.

This was accepted by S. But Barclays did not accept this outcome. They said the use of remote access software wouldn't be enough to justify declining the transaction requests. And they didn't think there were any other factors that would give them enough concern to decline the payment transaction.

An additional £21.43 was later recovered. But no agreement could be reached on the fair outcome for this complaint, so the complaint was passed to me to decide. Upon review I reached a different conclusion to the investigator. I issued a provisional decision that said:

Barclays has explained that due to the size of S as a business they do not meet the definition of a "micro-enterprise", so are not covered by the CRM code. A micro-enterprise is a business with assets or turnover less than €2million, and fewer than ten employees.

Having reviewed S' accounts with Companies House, I'm satisfied that S is a larger business than a micro-enterprise. The provisions on the CRM code would not apply to them. In any event the CRM code is designed to cover authorised push payment fraud, and the primary argument here is that S weren't aware payments were being made. In any event I've gone on to consider how the payments were carried out and whether Barclays should reasonably be responsible for refunding S.

Authorisation of payments

The relevant law here is the Payment Services Regulations 2017 (PSRs) – these set out what is needed for a payment to be authorised and who has liability for disputed payments in different situations. With some exceptions, the starting point is that the payer is responsible for authorised payments, and the bank is responsible for unauthorised payments. S says their employee didn't authorise the payments, but Barclays has concluded that they did, and so I'll address this point first.

It isn't in dispute that the fraudster tricked the employee of S into allowing remote access to the Barclays.net system, possibly using a spoof version of the real site. And it seems more likely than not the SWYS device was used to authorise several payment requests. The technical data supplied by Barclays confirms this is the case. So, S is the victim of a scam here.

I'm satisfied that the payment requests were correctly authenticated using genuine login details and completed using the SWYS device. Under the PSRs for a payment to be authorised, it must be consented to by an authorised individual, or someone acting on their behalf. This consent needs to be "given in the form, and in accordance with the procedure". In practice this in outlined in the terms of the account. Here the most applicable term is:

> *to make a payment or withdrawal from your account, you need to give us authorisation. You can do this in several ways...*
>
> > *Log onto Online Banking, the Barclays app or any other applicate Electronic Banking Service we provide using your security details. Follow the instructions to complete the payment.*

It's accepted that the fraudster set up the payment instruction in the Barclays.net system, using S' legitimate credentials.

I've also considered whether the payments could be considered authorised on the basis that the employee confirm the payment instructions using the SWYS device. Barclays have said it would have asked the employee to submit the payment transaction. But the employee at S believed they were only agreeing to reactivating cards.

As S Barclays.net was set up for dual authorisation, it would have required the payment to be set up with one set of account details, then authorised with another using the SWYS device.

I think it's more likely that not the SWYS device would have asked for the PIN and then presented a screen asking them to authorise a payment request, along with a date and time. This is what's displayed when a payment transaction is being submitted under the dual authorisation process, which was what was happening. And I've seen nothing to suggest the fraudster could have remotely manipulated the SWYS display. The employee would then

need to physically press "OK" on the device to confirm the submission on the payment transaction.

I'm persuaded that it's reasonable for Barclays to rely on this confirmation as consent by S to process the payment instructions. Essentially, I'm satisfied that it's reasonable to treat the payments as authorised. I don't see that under the PSRs or the terms of the account there is an obligation on Barclays to refund S.

However, I've gone on to consider what's fair and reasonable in all the circumstances of the complaint.

Should Barclays have done more to prevent the transactions?

In general, the starting position in law is that Barclays would be expected to process payments and withdrawals that their customer authorises them to make, in accordance with the PSRs and the terms of the account. But there are also legal and regulatory expectations that the bank will monitor accounts and payment activity to look for signs their customers may be falling victim to financial harm – such as fraud.

There is a balance to be struck between investigating significant numbers of transactions in details and allowing a customer to transact freely. But my expectation is that if a payment looks particularly unusual or high-risk, then the bank may choose to intervene and ask the customer further questions about the payment. The hope here is that this prevents any losses from going out.

Here though, I'm not persuaded that the batch payment itself stands out enough, such that Barclays should have intervened. S' account had regularly made batch payments of around this amount in the weeks before the fraud took place – for example just over £50,000 being send on 8 April. I'm also not persuaded that these were mostly new payees would stand out enough, such that I would reasonably expect Barclays to intervene.

The fact that the payments were made with dual authorisation – so requiring two staff members at S to approve the payments – would also help mitigate any concerns Barclays had about the funds potentially being misappropriated.

There was a later payment that was blocked – but this was attempted using the online banking system, rather than the Barclays.net payment system.

I've considered whether the use of remote access software should have given Barclays pause. But I don't see that this in itself would be enough for me to say Barclays should have declined to process the payment transactions – there can be many legitimate reasons for remote access to be used, particularly in the context of this being a business account. In the absence of any other concerns, I can't say Barclays missed any obvious signs that S' account was falling victim to fraud. Barclays didn't fail so significantly in their obligations to keep the account secure that they should reasonably refund S.

Did Barclays do enough to recover the funds?

I'm satisfied that Barclays contacted the receiving parties within a reasonable time – and I'm glad that some of the funds were available to be recovered. I've seen nothing to suggest that there were any unreasonable delays in the recovery attempt from Barclays.

Overall, I don't doubt this has been a difficult and stressful experience for the directors and staff of S. But I'm not minded that Barclays should be responsible for refunding their remaining losses.

This was accepted by Barclays. S responded to say that they didn't agree the use of the SWYS device did not constitute authorisation, saying it did not display the details of the transaction being made. They said in such a high-pressure situation the use of the device could not have combated the fraudster's narrative. They said even if it was to be consider authorised, there were enough risk factors that Barclays ought to have intervened. They didn't think the use of remote access software was typical of normal use.

It now falls on me to consider the evidence afresh.

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.

I appreciate this will be disappointing to S, but I remain satisfied with the conclusions reached in the provisional decision, for largely the same reasons.

In S' response to my provisional decision they have referred to various other decisions issued by our service. But each case is judged on its own merits, and while the circumstances may seem similar, I have to decide this case based on its own material facts.

In this case, I remain satisfied that the payments were authorised. As mentioned in the provisional decision, I accept the batch payments were likely set up by the fraudster using remote access given to them, which in turn allowed them to access the Barclays.net platform.

But from what we have been told, it was a staff member at S who confirmed the payment using the SWYS device. The device at the time would have shown that entering the PIN was to "authorise" a payment batch – this is what the standard wording for this on the SWYS device, and I've seen nothing to suggest the fraudster would have been able to remotely change or manipulate this screen.

From this it would have been reasonably clear that this was to authorise a payment batch. And the payment batch could not have been processed without the entering of the PIN and pressing enter. On that basis I'm satisfied that it's not unreasonable for Barclays to have treated this as consent to process the payment batch. I don't see on that basis that there is an obligation on Barclays to refund S.

In terms of monitoring S' account for signs of fraud or financial harm, I'm not persuaded that the batch payment was so significantly out of character for the account. As mentioned, it was in line with recent activity on the account in terms of amounts and being processed using the Barclays.net system. S has argued that the payment used up a considerable amount of the balance on the account, but looking through the history this wasn't out of step with how it had been used previously.

I've considered S' arguments about remote access carefully – but I wouldn't say that this should cause Barclays to block an account or decline any payments transactions. S has correctly pointed out that this is something Barclays look to detect, as it potentially could be an indicator of misuse. But I'm not persuaded by S' arguments that it is uncommonly used for business banking purposes.

I see it would be reasonable to take a detection of remote access into account when considering the risk – but here in the absence of any other obvious signs of fraud or financial harm, I don't see that Barclays should reasonably have done more. I'm also minded that the dual authorisation process – whereby two separate login details at S were needed to

authorise the payments – would mitigate concerns for Barclays more than the remote access would prompt them. On balance, I'm still not persuaded that Barclays were unreasonable in allowing the batch payment without further intervention.

Neither party commented on the recovery of funds, so I'm satisfied with the conclusions in the provisional decision on these.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask S to accept or reject my decision before 16 September 2025.

Thom Bennett
Ombudsman