DRN-4897299

The complaint

Mr W complains that Barclays Bank UK PLC hasn't refunded debit card transactions he says he didn't make or authorise.

What happened

I issued my provisional decision for this complaint on 5 March 2024 and both parties have now had an opportunity to respond. I've included a copy of the provisional decision at the end of this final decision, *in italics,* for reference. I won't otherwise repeat all the circumstances and findings set out within it.

Barclays responded to the provisional decision and accepted the findings.

Mr W didn't accept the findings and had some more points he wanted to raise. To facilitate his response, he was provided with copies of the evidence I relied on. That included technical evidence and data which showed an audit of the transactions in dispute.

Mr W has sought assistance from some computer science and security experts who have provided some responses on behalf of Mr W. But I'll mostly refer to Mr W throughout this decision, for the sake of clarity.

I won't set out in detail all the further arguments put forward by Mr W as they are well-known to all parties. Instead, I'll summarise the key themes:

- Barclays didn't have a proper mandate to debit Mr W's account and he can't be said to have authorised the transactions;
- Barclays failed in its duty of care to protect Mr W's account; *and*
- Barclays ought to have raised a chargeback.

I have already responded, in part, to these points. Mr W has since commented on them further. And it's now necessary to set out my findings in this final 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, and having included the submissions of all parties following my provisional decision in my considerations, I am reaching the same outcome as previously explained. Mr W's complaint is upheld in part.

Most of my findings and reasons for them remain the same as set out in my provisional decision, and so I won't repeat those here. I will address the newer arguments made by Mr W and explain why the outcome remains a partial uphold, with him to receive a partial refund of his loss.

I'll set out my findings under the same broad points used in the 'what happened' section above. And in setting out the findings in this way, and thinking about the content of what I will go on to say, it's important to note that I'm not specifically addressing every individual argument and suggestion made by Mr W. I have considered all that has been said, but my findings focus on the key issues that determine the outcome of the complaint.

Barclays didn't have a proper mandate to debit Mr W's account and he can't be said to have authorised the transactions

In my provisional decision I set out why I believed it to be more likely than not Mr W did authorise the payments himself, in terms of both authentication and consent. In doing so I set out a range of possible scenarios for how the disputed transactions might have been authorised or made without Mr W's knowledge. And it was in going through those scenarios that I arrived at Mr W having authorised the transactions as being the more likely than not explanation.

Mr W hasn't provided any further information or evidence that would lead me to a different conclusion. There's been nothing to suggest one of the scenarios I described (or any other) is more likely. And I note those assisting Mr W have also said they believe it's more likely than not the genuine card was used to make the payments (whilst also noting they've expressed the available evidence is limited). Considering this my position is unchanged.

The further arguments made by Mr W in respect of the mandate and whether he can be considered to have authorised the payments can be addressed in considering the effects of the Payment Service Regulations (2017).

Mr W argues Barclays didn't have a valid mandate to debit his account. This is on the basis that Mr W had reported the transactions as fraudulent before the payment settlement process was complete. Mr W says the impact of this is that his authority was withdrawn, and that Barclays no longer had his permission to debit his account.

However, the PSRs are clear on the withdrawal of consent, or rather that it isn't possible to withdraw consent for card transactions like the ones in dispute here. The relevant sections of the PSRs are regulation 67 (3) and 83 (1) & (2):

67 (3) The payer may withdraw its consent to a payment transaction at any time before the point at which the payment order can no longer be revoked under regulation 83 (revocation of a payment order).

83 (1) Subject to paragraphs (2) to (5), a payment service user may not revoke a payment order after it has been received by the payer's payment service provider.

(2) In the case of a payment transaction initiated by a payment initiation service provider, or by or through the payee, the payer may not revoke the payment order after giving consent to the payment initiation service provider to initiate the payment transaction or giving consent to execute the payment transaction to the payee.

Card payments are a form of pull payment that are initiated by or through the payee. That is – broadly speaking – what is happening when a card is inserted into a point of sale (POS) machine and a PIN is entered, with a transaction then being authenticated and consented to. I'm then satisfied, as per the PSRs, the mandate to debit Mr W's account was valid as consent couldn't have been withdrawn after the point the transaction was completed on the POS device, with Mr W's card having been inserted and his PIN entered each time.

It is possible that a transaction might be properly authenticated – and even processed – without it being consented to. That is typically what happens when an unauthorised transaction is made, whether that be using chip and PIN or by other means. A typical example would be if a thief shoulder-surfed someone using their PIN and then went on to steal the card, using it together with the PIN to make unauthorised transactions. I've already explained in my provisional decision why I don't believe such a scenario applies here, and why I believe the transactions were authorised by Mr W.

The further arguments made by Mr W focus on whether he can be said to have consented to the transactions if he didn't fully appreciate what was happening and hadn't intended to authorise the transactions or payment values that he did. This position is put forward in

response to my findings that he was more likely than not, tricked, without fully understanding that so many payments were going through and for such high amounts.

I've set out a useful point made by Mr W below, stated in the correspondence which followed the provisional decision and further discussions on authorisation:

However, authorisation is not a physical act; authorisation is the giving of permission, and giving permission requires intent.

I can understand where Mr W is coming from here. The suggestion is that someone must know all the details of a payment to properly authorise it. Or that Mr W needed to know the explicit details of each transaction and intended to make each one if he's to be said to have authorised them. And, if he didn't fully understand those details, or didn't fully intend for the payments to go through at the values they were set at, whether because he was being tricked or otherwise, then he can't be said to have authorised them. But this is not the position set out in the PSRs. The relevant sections here are regulation 67 (1)(a) & (2)(b):

67 (1) A payment transaction is to be regarded as having been authorised by the payer for the purposes of this Part only if the payer has given its consent to—

(a) the execution of the payment transaction

(2) Such consent—

(b)must be given in the form, and in accordance with the procedure, agreed between the payer and its payment service provider;

What's important here is that the PSRs determine the giving of consent to be defined as the completing of the form and procedure agreed between parties. The form and procedure is typically set out in a customer's account terms and conditions, as it is for Mr W. They state:

Asking us to make a payment

To make a payment from your account, you need to give us authorisation. You can do this in several ways, including the ones below.

• Present your card and enter the card PIN (or you may be asked to sign).

These are very common terms used by the banking industry, though wording may vary slightly. And the form and procedure for giving consent for a payment is clearly set out here. It's then fair and reasonable to say – given my findings on what more likely than not happened – that Mr W did give his consent for the transactions and that they are to be treated as authorised under the PSRs.

Barclays failed in its duty of care to protect Mr W's account

I set out detailed findings on this point in my provisional decision and I remain of the view that Barclays did fail to protect Mr W.

Mr W has suggested that Barclays ought to have intervened at an earlier point than I said, suggesting Barclays ought to have been on alert after the first or second disputed payment. He's said I should have taken account of features such as the merchant category codes, the time of day, and the short gaps between transactions, among other things.

I can confirm I did take account of all the characteristics suggested by Mr W. And my findings on the point Barclays ought to have stepped in remain the same. I'm not persuaded the earlier payments represented such a clear fraud risk that Barclays ought to have gone against its legal obligation to process authorised payments quickly.

Barclays ought to have raised a chargeback

Each different card scheme offers a chargeback process as a means of settling disputes between customers and merchants. It's important to note that a chargeback isn't a legal

right. Instead, it is a voluntary dispute resolution process put in place by the relevant card scheme. The card scheme sets its own chargeback rules which banks must follow closely.

We would expect a bank to raise a chargeback when there is a reasonable prospect of success. If it doesn't, and even though a chargeback isn't a legal right, we might consider a complaint and find that a bank ought to have raised one on the basis it would more likely than not have been successful. In such circumstances we might then find it would be fair and reasonable for the bank to compensate the customer for their loss.

The chargeback scheme rules describe when a chargeback can and can't be raised. And a bank shouldn't raise a chargeback when it looks likely to fail, perhaps on the off chance it might be successful.

Mr W reported the disputed transactions as unauthorised. That might be used as a chargeback reason. But, before raising a chargeback under that reason code, a bank should first consider whether that is the more likely than not explanation for how the transactions took place. That in turn informs whether the chargeback would have a reasonable prospect of success.

Given Barclays findings at the time it investigated the transactions, alongside my own findings that the transactions were authorised, I consider it was fair and reasonable to not raise a chargeback under this reason code.

Mr W has suggested a claim could have been raised on the basis of goods/services not being received. That would have been based on him having either received no good/services at all, or at least not to the value of what he was charged. But I'm satisfied Barclays acted fairly and reasonably in not raising a chargeback under this reason code too.

Within the relevant chargeback rules each possible reason code or dispute condition is set out, describing both the chargeback rights and what constitutes an invalid dispute. Under the goods/services not received dispute condition it states an invalid dispute includes '*A Transaction that the Cardholder states is fraudulent'.*

This is the claim that was made by Mr W – that the transactions were fraudulent, in that he'd not authorised them – and so the chargeback reason was invalid from the outset and couldn't be used.

Furthermore, the chargeback rules set out the requirement for certain information and evidence to be supplied by the issuer (Barclays) if a claim is to be made. Requirements relevant to Mr W's complaint include evidence showing:

- *Cardholder attempted to resolve with Merchant*
- *A detailed description of the merchandise or services purchased, unless prohibited by applicable laws or regulations. This description must contain additional information beyond the data required in the Clearing Record.*

Mr W couldn't fulfil these requirements and so a chargeback couldn't have been raised under the goods/services not received reason code. Mr W couldn't contact the merchant as he had no means of doing so. And he couldn't give a detailed description of what was missing as he didn't know what he'd been charged for. Note that for the chargeback to be raised, specifics must be provided. It's not enough for him to have said he was overcharged for drinks, or that the payments were for nothing at all. Nor could he have applied a broad description of 'professional service', one of the merchant category codes recorded against some of the disputed payments. That would not have been enough detail for a chargeback to have been successful.

It isn't surprising that Mr W couldn't provide this information, given the circumstances of the complaint. But those broader circumstances don't mean that an otherwise invalid chargeback reason would become useable.

Where there is no valid reason code that can be used, a chargeback can't be raised. It wouldn't make it through to the point at which a merchant was challenged to provide evidence to counter the claim. And so the prospect of success of an otherwise valid claim can't be considered.

Mr W has said that Barclays ought to have at least sought further information from the merchants so that a more informed position could be reached and a properly explained chargeback claim raised. There is a stage in the chargeback process before a full claim is raised, known as a retrieval request. The expectation here is that the merchants would have either automatically conceded and refunded Mr W or that no response would have been received, putting Mr W in a strong position to raise a chargeback.

I've considered this but it doesn't lead me to conclude Barclays should refund Mr W. What I've said about the chargeback reasons codes being invalid still stands and would do even if Barclays requested further information from the merchants via the chargeback process. It made a fair and reasonable decision at the time to not pursue a chargeback, and that decision remains fair and reasonable now.

Putting things right

Should Mr W accept this final decision Barclays must:

- Refund 50% of all transactions made after 9:27am (GMT)/6:27am (local time) on 18 March 2022 – totaling £9,039.46; *and*
- Pay interest at 8% simple per year, calculated from the date of loss to the date of settlement. I've awarded this interest payment as I'm satisfied Barclays ought to have prevented the loss at the time, and so Mr W has been deprived of the funds since the date each payment was made.

My final decision

I uphold this complaint against Barclays Bank UK PLC in part.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 16 August 2024.

My provisional decision – issued 5 March 2024

I've considered the relevant information about this complaint.

My findings and the outcome I've reached are different to those of our investigator.

I'll look at any more comments and evidence that I get by 19 March 2024. But unless the information changes my mind, my final decision is likely to be along the following lines.

The complaint

Mr W complains that Barclays Bank UK PLC hasn't refunded debit card transactions he says he didn't make or authorise.

What happened

In setting out the background to this complaint I won't be including a timeline of all events that transpired. Some of that detail isn't necessary, though I have considered everything that's been said by both Mr W and Barclays. My decision focuses on the key events that affect the overall outcome of the complaint.

Mr W was travelling in South America in March 2022. He's described how he met some new friends, and they took him to a bar (I'll refer to it as Bar T) on the night of 18 March 2022. Mr W spent the evening there and says he bought a few drinks, perhaps some food, before returning to his hotel (which was around five minutes away by taxi, 15 minutes on foot).

Mr W has said he returned to the bar on other nights. He doesn't think he went on 19 March but did on 20 and 21 March. He's said he wasn't with the new friends on at least one of these occasions.

On 21 March 2022 Mr W saw a notification from Barclays on his phone. This was hours after he'd left Bar T, having gone to bed in the meantime. The notification said there was a pending transaction for around £1,500. Mr W didn't recall authorising such a transaction and so checked his online banking. It's at this point Mr W discovered a large number of transactions that had either already been fully processed or that were pending but that he didn't recognise. In total, there were 18 transactions he didn't recognise, spread across the four days from 18 to 21 March 2022. Each payment was between £391.39 and £2,348.34. The total amount in dispute is £19,810.53. There were three different merchant names, aside from that of Bar T, connected to the disputed payments.

Mr W contacted Barclays to report that something was wrong. He had difficulty in getting the dispute fully logged, and in gaining any kind of clear understanding from the bank as to what had happened. It took a long time and multiple calls before Mr W had a better understanding of all that was in dispute. He says the bank's lack of clarity, combined with the fact his phone was stolen on 24 March 2022, meant he had no option but to return to the UK to try and sort things out.

Barclays investigated once the claim was fully logged. But it said it wouldn't refund Mr W. Barclays said all the transactions were authorised using the genuine card and PIN. It could tell the genuine card was used because the integrated chip had been read for each transaction and so found there was little explanation for how the transactions could have been made without Mr W's authority.

It noted Mr W had said the card used for the disputed transactions had always been in his possession, meaning it hadn't been stolen by an unknown fraudster. Barclays said, if that were the case, it would have meant that someone was able to take, use, and replace Mr W's card numerous times without him noticing. And that this person (or persons) would also have had to gain knowledge of Mr W's PIN.

Barclays said that if that had been allowed to happen, then it clearly demonstrated that the card and PIN hadn't been kept secure.

Mr W was unhappy with Barclays' response and so brought his complaint to our service. One of our investigators considered the circumstances and said Barclays had acted fairly and reasonably, so didn't uphold the complaint. Mr W has since asked that an ombudsman review the complaint and so it has been passed to me to consider.

What I've 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.

I intend to uphold this complaint in part, with each party bearing some responsibility for the loss. I'll explain why.

In cases like this it will never be possible for this service to determine exactly what has happened. It's the case that evidence and information will often be incomplete. I must use what is available to reach what I consider to be the fair and reasonable outcome in all the circumstances of the complaint. In doing so I will reach my findings on the balance of probabilities. And where there is a dispute, I'll use the available evidence to decide what I consider is more likely than not to have happened.

Were the transactions authorised by Mr W?

The starting point at law is that a customer is responsible for any transactions made from their account which are properly authorised. This is set out in the Payment Service Regulations (2017) and confirmed in Mr W's account terms and conditions.

Where there is a dispute over the authorisation of payments, as there is here, a firm must be able to evidence that it is more likely than not the customer made or otherwise authorised the payments. And, for plastic card complaints like Mr W's, it isn't enough for a firm to rely only on evidence of the chip and PIN being used.

There are two important parts to authorisation – authentication and consent. I'll address each separately.

There is also a consideration of gross negligence to be applied. This only comes into play when a transaction is deemed to be unauthorised. There would be an acceptance – or a finding – the customer didn't make or otherwise authorise the payments themselves, but where they've demonstrated a significant degree of carelessness. In this case it would mean an assessment of whether Mr W had taken proper care of his card and PIN.

Authentication

Authentication is essentially the technical part of a transaction and the mechanism used to debit a customer's account. Here, Barclays has demonstrated that the authentication method used was chip and PIN. The electronic record of the transactions it has provided do evidence this. I find this evidence to be persuasive in establishing that Mr W's genuine card and corresponding PIN were used to make the transactions.

I know Mr W was initially told, when reporting the disputed payments, that it looked as though the magnetic stripe was read. I'm not sure why he might have been told that, but I've seen no such evidence it was the case.

The subject of card cloning has been referred to. But I'm not persuaded that explains what's happened here. Broadly speaking, there is little evidence to suggest the integrated chip in a card can be cloned or copied for use in everyday situations.

This is different to magnetic stripe cloning, which is very much possible. But where cloning of that nature takes place, the electronic record will show the magnetic stripe was read. And so such instances are easy to identify.

The evidence to support a lack of cloning here goes beyond the bank's own records. This service looks beyond what might be technically recorded and will always consider the broader circumstances alongside the customer's version of events. Those broader considerations and the pattern of transactions don't support that a fraudster had managed to clone Mr W's card.

Had they done so, I'm satisfied the usage of the card would have been more rampant from the outset. That's because the fraudster would be looking to maximise the amount of money they could get before being discovered. What can be seen in Mr W's case are clearly some high value payments made in quick succession. On the first day there are four disputed payments that are successful. There are five others that are approved but then reversed, one for as much as £2,348.34. So clearly spending – and attempts to spend – is high. But, after a successful payment of £782.78 at 7:03am, there are no other attempts to use the

card until the following day. And there are no attempts to withdraw cash. There were still funds available in the account.

The same pattern is then repeated on 19, 20, and 21 March. Again, there are high value and high frequency transactions. But the attempts at using the card are confined to a specific period of time – around 5:30am to 7:00am (Brazil local time). There's little in the way of persuasive explanation as to why a fraudster, armed with a working card and PIN that they could use whenever and wherever they liked, would restrict themselves to only transacting in such a small window, and using only a specific set of merchants.

It is possible a fraudster might look to avoid detection by spreading out activity over a few days. But that risks detection. A victim would only need to spot one unauthorised transaction, with the card subsequently being cancelled, and the opportunity for the fraudster to obtain more money would be gone.

It is also the case that the card does track back to the same location each day. And on some of those days there is undisputed spending at Bar T, which Mr W has confirmed being at. He also believes this is the likely venue at which the disputed card spending took place, although he isn't sure how it happened.

I would agree that it seems Bar T was the likely point of compromise here, given what Mr W has said about his movements. But I don't consider it a likely explanation that a fraudster with a cloned card would have been returning to the same spot at which the fraud commenced, and at the same times as Mr W. And so, Bar T and the different merchants used repeatedly afterward don't support a cloned card being in use.

It's for these reasons I'm satisfied Mr W's genuine card was used alongside his PIN. And so, the authentication of the disputed payments is sufficiently evidenced by the bank.

Mr W has suggested he may have been the victim of what's sometimes known as a 'pre-play attack'. But I'm not persuaded this is what happened. The theory behind such an attack can be summarised as a scenario where the point-of-sale terminal a merchant uses is tampered with (perhaps without the merchant being aware) by fraudsters. The fraudsters then essentially hijack a payment that's being genuinely executed and use the technical features of the card and transaction data to create new fake payments for processing. These transactions aren't made using the physical card and PIN. They're made to look like they are, to trick the system. It might be that these transactions are queued up, to be executed at different times to appear less suspicious. And the amounts may even vary.

The transactions in dispute here only ever occur in batches between Mr W's genuine spending. There is never any overlap from one day to another. As an example, Mr W genuinely transacted at Bar T on 18 March 2022 at 05:53am. The disputed transactions then begin at 06:19am and stop at 06:31am. Mr W then transacts again genuinely at 18:10 (06:10pm) on the same day using his card, and there is continued card usage right through to 5:29am the following day before the disputed transactions start again. There's then a further genuine transaction at 06:45am on 19 March 2022. This same pattern is repeated over the course of the remaining disputed transactions.

I accept it's possible that a fraudster could have queued up transactions for the same kind of time of day. But I don't believe that's the more likely than not explanation. More likely would be that the genuine card and PIN was being used again at the same location each time. A location Mr W has confirmed he was at on at least three of the relevant days.

There is further evidence to show a pre-play attack isn't the more likely than not explanation. I've seen the bank's technical evidence that confirms Bar T and the three other merchants all had unique terminal IDs. That suggests that there were four different terminals used across Mr W's genuine spend at Bar T and the three merchants involved in the disputed transactions. The use of each different merchant and terminal is interspersed amongst the others. Each different merchant and terminal is sometimes used within minutes of each

other, in various combinations. This would mean that all terminals would have to have been affected and be coordinated in the same attack.

I've also seen evidence of all transaction authorisations being received sequentially by Barclays. This means the transaction counter for each payment made using Mr W's card is received in order, with a unique counter ID and cryptogram. Had transactions been generated in bulk and released over time it would be expected for this counter to be out of sequence because of any genuine card spending. That it isn't is further evidence to support that a pre-play attack hasn't occurred and in turn that same evidence shows the payments were properly authenticated.

As a final point, there also appears to be direct interaction from the merchants at times, with payments being reversed or refunded. I can't say why that happens. But it doesn't suggest there's a series of payments lined up ready to be executed as the reversal of those payments would likely also have to be set up at the same time. That might be possible, but it seems improbable.

Did Mr W consent to the payments being made?

Even where a payment is evidenced as having been properly authenticated a firm, like Barclays, must be able to persuasively demonstrate that a customer consented to it. That doesn't mean CCTV of the customer carrying out the transaction(s) – or similar – must be obtained. It's a consideration of different sources of evidence. That will include how the payments were authenticated, as that provides a useful starting point in determining just how a payment could have been made without the customer's consent. Questioning how an unknown fraudster might have been able to use a customer's card and PIN without their knowledge is entirely valid in determining and evidencing authorisation. But there must also be an acknowledgement that a customer may have little to no idea how such a thing might have happened, and that doesn't necessarily mean they must have consented or that they should be held responsible for payments in dispute.

It's therefore important to take account of the wider circumstances and consideration must be given to the customer's version of events.

A helpful approach to considering consent is to address the possible explanations for how the payments might have been made, and by who. From there I can determine which is the more likely than not scenario. This then meets the requirement to assess the complaint on balance.

I'll come on to set out the possible scenarios in a moment. But there are certain findings of fact that I will make now, as they apply to multiple scenarios.

Mr W has said he would definitely have been in bed at the time of the disputed transactions. In early submissions the suggestion was he'd have been back at his hotel hours before the payments were made. But having considered the timing of both disputed and genuine transactions I'm persuaded that couldn't have been the case.

There are genuine transactions very close to some of the disputed ones. These include genuine spending at Bar T around 20 minutes before the disputed spending starts on 18 March 2022. A similar situation is evident on 19 March 2022 with genuine spending at a bar shortly before the disputed transactions begin. Also on 19 March 2022 is a genuine transaction at a pharmacy 17 minutes after the final disputed one. And, on 20 March 2022 a genuine transaction takes place at Bar T about 40 minutes before the disputed transactions begin.

I've put these timings to Mr W for comment. He still believes he was back at his hotel when the disputed transactions occurred. He's highlighted that his hotel was only a five-minute drive or fifteen-minute walk from the bar, so he could have made it back there before the disputed spending began. And, for the genuine spending that occurred after the final

disputed transaction on 19 March 2022, Mr W suggests he may have briefly left his hotel to purchase something like medicine for an upset stomach.

However, I'm persuaded it is more likely than not Mr W was still out and wasn't at his hotel at the time the payments were being made. Whilst the timings do make it possible for Mr W to have carried out genuine spending and travelled to or from his hotel before the disputed ones start and finish, it isn't the more likely than not explanation. That is reinforced by my findings on authentication, which place Mr W's genuine card – and by extension Mr W – as being with the merchant(s) that were processing the payments.

Mr W has pointed to Bar T as the likely place where the disputed activity occurs. That seems a reasonable conclusion to draw given his recollection of his movements. And it's also supported by the fact there were genuine transactions at Bar T on two of the four days that disputed payments occur. Mr W has said he doesn't think he went to Bar T on one of the days, and thinks his new friends weren't with him on at least one occasion. It does remain a likely point of compromise, though I can't say for sure. It's also possible Mr W visited a different establishment that he doesn't recollect. There's no way for me to determine this point beyond doubt. But ultimately, I don't believe it affects the overall outcome, for reasons that will become clear as I continue to set out my findings.

There are five potential scenarios that might explain how the disputed transactions were made:

- *Mr W's card was cloned, and his PIN obtained by unknown means;*
- *Mr W's card and PIN were used to execute a pre-play attack;*
- *An unknown fraudster was able to take, use, and replace Mr W's card;*
- *Mr W authorised the payments himself and denies doing so;*
- *Mr W was tricked into authorising more payments than he intended to, and for greater amounts.*

I'll address these possible scenarios in turn. In doing so, it's important to consider the findings already made on authentication. There is some natural overlap.

Mr W's card was cloned, and his PIN obtained by unknown means

I've already addressed this scenario when considering authentication and I've explained why I don't believe a cloned card was being used. I won't repeat those findings here.

Suffice to say that the pattern of transactions doesn't suggest that an unknown fraudster had unfettered access to a cloned card, with working PIN, that they could use wherever and whenever they wanted.

It's also true there were no failed attempts to use the card once it was cancelled. A fraudster in possession of a cloned card wouldn't have known that the card was no longer working and would more likely than not have tried to sue it again. But that didn't happen.

Mr W's card and PIN were used to execute a pre-play attack

I've also explained this scenario in the section on authentication. And the same logic carries across to the question of consent. It's not impossible that a pre-play attack was what happened here. But, based on the information and evidence available, I'm not persuaded it is the more likely than not explanation. The timings and pattern of the transactions, that they are spread over four days, the lack of overlap with genuine spending, Mr W's movements, and the bank's technical evidence do not point to this scenario being more likely than the others.

I've also questioned whether there is any record of similar claims against the same merchants, and there appears to be none. If a fraudster had gone to the trouble of setting up

the conditions for a pre-play attack, then I'd expect there to be evidence of multiple claims from numerous customers, all bearing common features. But I've seen no such evidence.

An unknown fraudster was able to take, use, and replace Mr W's card

Mr W has confirmed his card was never out of his possession, or at least he never noticed it being so.

This scenario would require no technical knowledge or ability to execute, unlike the first two scenarios. Someone would have to gain knowledge of Mr W's PIN, but that might be explained by shoulder surfing or a hidden camera, for example.

Mr W has said how he suspects the people he became friendly with (that took him to Bar T originally) might somehow have been involved. But he's also said they weren't with him every night. So they wouldn't have had the opportunity to take and replace the card.

It's possible a completely unknown fraudster might have shoulder surfed Mr W. However, it doesn't seem plausible that someone would be able to take and replace Mr W's card with such frequency as would be required, on so many occasions, over so many days, without him ever noticing. And Mr W hasn't identified anyone else that was spending hours with him each night for four nights. It would have to have been someone he was in close proximity to and/or familiar with in order to execute the take and replace each night.

Why such a fraudster wouldn't keep the card on day one, so that they might carry out as much spending as possible, lacks reasonable explanation. It seems unlikely such a person would expect Mr W to return to the same spot so that the same pattern of take and replace could be executed again. And, as with other scenarios, the longer the disputed transactions were stretched out for, the greater the chance of discovery.

Mr W authorised the payments himself and denies doing so

Mr W's version of events has been consistent from the point at which he reported the disputed transactions to Barclays. It's also evident that he was taken aback by the volume of transactions and the amounts that had been processed (both cumulatively and for individual payments).

That he hasn't been able to explain exactly how the disputed payments happened doesn't mean he is automatically assumed to have consented to them, or that he knew all about them.

The pattern of the transactions does not look like one someone would willingly carry out. And the involvement of three to four (if Bar T is included) merchant terminals, all being used at the same time, suggests to me that something underhand was happening without Mr W's full knowledge.

There's no evidence to show Mr W checked his balance or had any other means of knowing about the disputed payments until he logged into his online banking on 21 March 2022. This means there's nothing to suggest he was aware of what was happening on each day, or that he was checking to see which payments were going through, how much money was left, or anything else to suggest he was a completely willing participant in the spending.

It's difficult to conceive of a scenario in which the payments were entirely legitimate. I don't believe Mr W has knowingly transacted in this manner and then simply denied it.

Mr W was tricked into authorising more payments than he intended to, and for greater amounts

This to me is the more likely than not explanation for what happened. A combination of Mr W's version of events and the other available evidence point to that being the case.

I've mentioned above the suspicious nature of the transactions. It's clear they are made in quick succession and for significant sums of money. Some of those sums are repeated across each tranche of transactions. At other times the amounts vary substantially.

I've also considered that the transactions occur across three different merchant terminals (not counting the Bar T terminal), often within seconds of each other. That suggests the card is being switched between point-of-sale terminals quickly to process more payments.

I've also taken account of the fact that the registered merchant codes linked to each terminal don't marry up to a bar or entertainment venue. One might, at a stretch, meet that criteria, where the merchant is described as engaged in lodging (hotels etc). But the other two are broadly unclassified. Where the relevant card scheme gives examples of what the merchant codes link to, they are not even closely related to a bar or entertainment venue.

These facts suggest to me that there were nefarious parties involved in the processing of the payments. But, for reasons I've already set out in ruling out other scenarios, I'm persuaded Mr W was involved too, albeit unwittingly.

It's not an unknown for staff at bars to be involved in crime. This can involve the tricking of customers in various ways. That might be by hiding or disguising the amount of a transaction, so the customer consents to it without knowing the true value of the payment.

Or a bad actor might say that a payment hasn't gone through when it has, thereby encouraging the customer to authorise a further transaction. The variations on this type of trickery are too numerous to list here. And different methods can be combined, as was probably the case here. What's key is that the evidence and information available does point to that being the more likely than not explanation.

These tricks employed by underhand staff often mean the customer is left with the card in their possession at the end of the night, as was the case here. It often means the customer has no idea of the true volume and value of the transactions, as is the case here.

Mr W's version of events suggests that he would have carried out more than one transaction at Bar T each night. He's described staying there for a while, buying several drinks, and perhaps some food. And yet there are only two transactions directly attributed to Bar T. Those are for small amounts and on different nights. On the occasions they occur, the payments are made before the disputed ones began. It's then quite feasible the subsequent transactions were made by Mr W when he believed he was settling a bill, giving the bad actors an opportunity to target him. It's equally feasible all transactions made on days without the initial Bar T payment were instances where Mr W thought he was making a legitimate payment but where he was in fact being tricked.

There is also some further evidence that this is a more likely than not explanation for what happened. It's found in Mr W's account history where I understand he had a very similar thing happen to him in Madrid. It's possible this is completely coincidental and circumstantial. But I can't ignore the fact something like this has happened before, suggesting Mr W might be susceptible to such trickery.

On the night of 31 January 2022 Mr W was encouraged into a bar in Madrid, having already been out drinking for some time. The next day Mr W saw that around £2,000 was due to come out of his account. He had expected maybe around £300 to debit.

I've listened to the call recording where Mr W contacts Barclays about the pending payments. It becomes clear that Mr W had little understanding of how the payments had come about, and he questioned authorising them. But it also became apparent in the call that Mr W was very unsure of exactly what had transpired the night before. For one, he thought he'd left the bar around 3am. But it was clear from the timing of the transactions that he'd been there until after 6am. That's a substantial difference and would seem to be double the amount of time Mr W believed he'd been there.

The timing of those transactions was confirmed in the call with Mr W, as was the method of authentication – ApplePay. I'm not making findings about any possible claim of fraud on those funds. But the facts are that many of the payments would have required either Mr W's

FaceID or his passcode for approval. But Mr W said he had no recollection of making as many payments as were processed, or for the values charged.

In the same call Mr W describes how he was buying drinks for various people he only met at the bar. He's also described how, when 'ten sheets to the wind' and having 'imbibed' a lot he likely wouldn't have been checking transaction amounts. He essentially accepts in the call that he was likely tricked at the bar.

There are clear parallels and similarities to this dispute. The payment method is different and, arguably, more involved as it required the card and PIN to be used and so perhaps more likely to be noticed by Mr W. But the common features are too striking to ignore. The transactions are late at night/in the small hours of the morning. And they seem to come after several hours of drinking alcohol. Mr W's recollections of how long and how late he'd been at the bar are shown to have been a few hours adrift – not an insignificant period of time – in both the Madrid and Brazil incidents.

We do then appear to have two distinct occasions where Mr W had been out for a long period of time and has subsequently had only partial recollections of what exactly he was doing. In the call recording from the Madrid incident Mr W confirms that, after a few drinks and being in good company, he probably wouldn't have been checking the transaction details, assuming everything was ok.

It might be argued that Mr W was less likely to fall victim to this kind of deception if he'd previously experienced it. But the evidence around transaction frequency and authorisation would suggest otherwise.

Given all the circumstances of the case, in consideration of all the evidence, and taking account the potential authorisation scenarios, I'm persuaded this is what is more likely than not to have happened.

It should be noted here that the kind of deception and trickery I've described doesn't affect the position on authorisation. Even where Mr W may not have been fully aware of what was happening, or what he was authorising, he is still deemed responsible having completed the authorisation process.

I'll also add that I would more likely than not still reach the same finding here, even without the details of the Madrid incident. But where that information is available, it does make it a more persuasive explanation.

Is it necessary to consider gross negligence?

Where there has been a finding that a customer authorised payments there is generally no need to go on to consider gross negligence. It only applies to situations where there's persuasive evidence that a customer didn't carry out – or otherwise authorise – transactions themselves.

But here, I'm going to comment on it for two reasons. For one, Barclays said in its final response letter, where it answered Mr W's complaint, that it felt he must have acted with gross negligence in not keeping his card and PIN secure. Second, it must be accepted that my finding on authorisation could be wrong, though I'm satisfied it is the correct on balance finding. If I am wrong, and someone else carried out the transactions without Mr W's consent, then a consideration of gross negligence becomes relevant.

The consideration of gross negligence here means thinking about whether the evidence shows Mr W did or didn't take proper care of his card and PIN. The bar for a finding of gross negligence is a high one. It must be demonstrated that Mr W's actions went beyond ordinary carelessness.

If the evidence shows that to be the case, then Mr W can still be held responsible for transactions he didn't authorise. This is confirmed in both the Payment Service Regulations (2017) and Mr W's account terms and conditions.

I've already described many of the important factors within the circumstances and evidence that influence the outcome of the gross negligence consideration. For instance, I'm persuaded Mr W was at the venue at the time the transactions took place, that a cloned card wasn't being used, and that Mr W's PIN was entered correctly for each transaction. The different merchant terminals and pattern of transactions also play a part here.

I've already explained why I don't think the take and replace scenario is likely. And that would involve a situation where Mr W didn't know his card was in another person's possession. But there is a possible variation on this scenario, perhaps where Mr W gave his card over for a payment to be authorised and it was subsequently abused. Mr W has said that this never happened; that he never started a tab or gave his card and PIN to anyone. But I've still considered it as a possibility.

Such a situation might arise, for example, if Mr W had become trusting of the people he was with. Or it could be a case of the person processing the transactions saying a payment hadn't been successful and so took the card away to try again, having also obtained the PIN (and even where Mr W might not have been explicitly aware of that). As with previously described scenarios, there are too many possible variants to go through them all.

But the common fact that would have to apply would be that Mr W allowed his card to be in someone else's possession, with that person having had access to his PIN. The access to the PIN might have come about through Mr W's explicit disclosure of it, or it might have been observed without him being entirely aware. I'm not making a finding on how the PIN might have become known to the person putting through the unauthorised payments. That's because there is no change to the resulting outcome, regardless of what happened.

I'm satisfied Barclays position of stating such behaviour would constitute gross negligence is fair and reasonable. It would have meant Mr W knowingly allowing the card to be removed from his possession and with no way of knowing what might be done with it. And it would also have been reasonably foreseeable – to varying degrees, depending on the circumstances – that the person with the card would also have knowledge of the PIN. What I mean by that is if Mr W disclosed his PIN to someone then it would be obvious they had it to use alongside the card. But even if Mr W didn't explicitly disclose it, it was still foreseeable that they might have observed him entering it for a genuine or attempted transaction.

In making that finding it's important to consider the transaction timings. These demonstrate that Mr W would have allowed the card to be out of his possession for anything up to 30 minutes, seemingly with no knowledge of what it was being used for. It would also mean Mr W never checked what payments were being processed, whether that be by checking his online banking or asking for receipts. The combined factors would then lead to a position where Mr W had acted with gross negligence and so could be held responsible for the transactions he's disputed.

Did Barclays act fairly and reasonably in allowing the payments to go through?

I've already explained the starting point at law on liability for payments in terms of both authorised and unauthorised transactions. But that isn't the end of the story.

I'm satisfied that, taking into account longstanding regulatory expectation and requirements and what I consider to have been good industry practice at the time, Barclays ought fairly and reasonably have been monitoring Mr W's account for possible fraud and the risk of him being caused financial harm. And, in doing so, it ought fairly and reasonably have taken additional steps, carrying out additional checks on payment instructions received, before processing those payment instructions where suspicious and unusual account activity occurs.

Barclays hasn't argued that such expectations aren't in place. Instead, it has said that it had no reason to question the payments given they were authorised using Mr W's genuine card

and PIN. But I'm not persuaded that was enough as that doesn't take any account of the wider circumstances, notably the frequency and value of the payments.

Relying on the card and PIN solely to assess whether a customer is at risk of financial harm is insufficient. It doesn't take account of a huge range of scenarios where the customer could be at risk whilst the card and PIN is being used, whether they are authorising payments themselves or where a fraudster is acting, having obtained the card and PIN. And there was no way for Barclays to know if Mr W was in such a scenario without suspending a payment instruction and questioning him about it.

Mr W clearly used his card and PIN a lot for spending, and frequently overseas. But the speed at which the disputed payments were put through, one after another, and the value of them ought to have caused Barclays alarm.

I'm satisfied Barclays ought to have recognised something was wrong on 18 March 2022 at the fourth attempt to use the card. By this time there had already been three transactions processed within eight minutes of each other, for values of: £547.95, £391.39, and £782.78. Each of those transactions was of a greater value than Mr W would normally transact for. And they are made very close together. It's also the case that two different merchants were being transacted with at the same time.

The fourth transaction, the one where I'm satisfied Barclays ought to have stepped in, was processed 90 seconds after the third. It was for £2,348.34 and to one of the same two merchants. This payment was reversed 30 minutes later, according to Barclays, because of something attributed to the merchant; it's unclear why the payment didn't debit Mr W's account in the end. But Barclays did receive it as a payment instruction, and so it does factor into the developing picture available to the bank at the time.

That fourth payment was clearly very high in value. And that value had escalated significantly on the previous three. The speed at which it follows the previous payments can fairly and reasonably be described as unusual and suspicious, and certainly a common indicator of fraud or risk of financial harm. It's somewhat difficult to imagine a legitimate scenario in which card spending like this would be genuine. But Barclays didn't intervene here to question Mr W about what was happening. In fact, it never did over the course of all the payments, despite further high value transactions being attempted in rapid succession and the introduction of a third merchant. For further context here, there were three more payments put through within two minutes of that fourth transaction. The lowest value was £1,878.67, the highest £2,661.45. But Barclays didn't consider Mr W might be the victim of fraud or at risk of financial harm and didn't step in to check that wasn't the case. I don't find that to have been fair and reasonable in the circumstances.

I'm therefore satisfied that Barclays ought to have intervened. It should have frozen the card and either attempted to contact Mr W directly or awaited contact from him. The question is then whether intervention would have made a difference. I'm persuaded it would have done.

I've already explained my findings on authorisation and gross negligence and what I consider is more likely than not to have happened. Within those scenarios I can see no reason why intervention from the bank wouldn't have prevented further loss to Mr W.

The nature of the situation would more likely than not have been revealed to him had the bank talked through the payment instructions it had received. If Mr W was being tricked and manipulated into making the payments, then the deception would have been uncovered. If Mr W's card was in another person's possession, with transactions being executed without his knowledge, he would have been made aware of them. Mr W would have been able to remove himself from whichever scenario he was in, and Barclays could have maintained the block on his card until he was in a secure environment.

I'm satisfied Barclays ought to have intervened, and that an appropriate intervention would have prevented further loss to Mr W. It's then fair and reasonable that Barclays ought to compensate him for that loss.

What proportion of Mr W's loss should be reimbursed?

I've made the finding that Barclays should bear responsibility for Mr W's loss. But his own actions can't fairly and reasonably be ignored. My findings also state that he must have – to some degree – been involved in the payments. And so, we have a situation where both parties ought to bear responsibility for the loss, for different reasons.

I'm satisfied the fair and reasonable outcome here is then for the loss to be shared equally between the two parties. That fairly accounts for the actions of both Barclays and Mr W.

Mr W will bear sole responsibility for the first three transactions, as I'm not persuaded Barclays needed to question those.

Putting things right

Should both parties accept the outcome, my direction will be for Barclays to:

- *Refund 50% of all transactions made after 9:27am (GMT)/6:27am (local time) on 18 March 2022 – totaling £9,039.46; and*
- *Pay interest at 8% simple per year, calculated from the date of loss to the date of settlement. I've awarded this interest payment as I'm satisfied Barclays ought to have prevented the loss at the time, and so Mr W has been deprived of the funds since the date each payment was made.*

My provisional decision

I intend to uphold this complaint against Barclays Bank UK PLC. I'll give until 19 March 2024 for any final evidence and information to be submitted for consideration before I issue my final decision

Ben Murray
Ombudsman