DRN-5045074

The complaint

A company which I will refer to as 'H' complains that Barclays Bank UK Plc is acting unfairly by refusing to refund the loss H suffered due to fraudulent transactions on the accounts it has with the bank.

Section A: What happened

H is a care home business providing residential nursing care facilities. It has been a customer of Barclays for several years. Miss Z is a director of H and one of the signatories of the two accounts that are relevant here.

On 12 December 2012 around noon Miss Z received a call from someone who later turned out to be a fraudster.

Miss Z says that the caller claimed to be calling from Barclays' fraud team and wanted to discuss recent transactions on her business debit card. The caller mentioned payments to Domino's Pizza for £12.99 and £5.99. Miss Z could see the £5.99 payment as a pending transaction on H's account. As regards the other, she was told that although it wasn't showing as a pending transaction, it had been made but was being withheld as suspicious. Miss Z told the caller that she didn't make those transactions.

In addition, Miss Z says that the caller referred to a genuine payment of £4,640.42 made from the account earlier that day, without her disclosing it. That suggested to her that the caller had a live view of the company's bank account, which only the bank would usually have. The caller also named some of the employees of the company and correctly mentioned how much wages were paid to them. So, Miss Z thought he was able to look through the bank account. All of this meant that she was convinced that she was talking to the bank.

Barclays says that at around the same time (at 12.06 pm), it sent a text to Miss Z. This was received in an existing (genuine) thread with Barclays. The message said that the bank needed to confirm 'some recent spend' in the debit card and asked Miss Z to reply to a number quoted in the text.

The bank then sent a second message at 12.10pm. This message said:

> "*£12.99 at DOMINO'S PIZZA was DECLINED, £5.99 at DOMINO'S PIZZA, £60.85 at [*another company name*]. If you made all the payments above please reply Y, if there are any that you didn't make please reply N*. "

Miss Z says she received both the texts at 12.10pm. She says that these messages which she received from Barclays in an existing thread reinforced what the caller told her. These messages further strengthened her belief that she was talking to Barclays.

Miss Z says that the caller wanted to help her with this issue. However, she was busy and as the 'bank' had already identified the suspicious transactions and taken steps anyway, she

asked him to call later in the day.

The caller agreed to call back later but also told her that he would cancel the debit card meanwhile. He further said that she would receive automated messages from Barclays, and she should ignore them as he was helping her and replying to the automated messages could create confusion.

The call ended at around 12.13pm. Soon after, at around 12.25pm Miss Z received an automated call from Barclays exactly as the caller advised. This was a genuine call from the bank. Miss Z says that she didn't answer it as she was busy (which was why she asked the caller to call back later).

The bank sent a text message at 2.36pm that it had temporarily stopped her card to protect H against fraud, and asked Miss Z to contact the bank. This message reinforced Miss Z's belief that she was in fact talking to the bank earlier in the day and that the bank's staff was following their assurance to help her. She says that she didn't call the bank as she was expecting a call from the bank soon anyway.

Thus, this was a sequence of events where the fraudster was able to match what he said with genuine actions from Barclays.

At 3.13pm, Miss Z took the second call from the fraudster. The fraudster told her that since they last spoke, there had been numerous fraudulent activities on H's account. Miss Z says that she panicked on hearing this, but the caller assured her that Barclays would take care of it and refund those transactions.

Barclays' records and Miss Z's internet history indicate that at around 3.15pm someone logged into the online banking (OLB). It doesn't appear that the fraudster had access to Miss Z's computer at that time. So, it seems more likely that it was Miss Z who logged into the OLB.

Miss Z was then instructed to download a software called AnyDesk on her computer. She says that the caller told her this was an anti-virus software to investigate whether there was any malware on her computer. In reality, this allowed the fraudster remote access and control of Miss Z's computer. Miss Z says that shortly after the software was downloaded, her computer screen went blank. She assumed that this was part of the virus check the caller had described.

The fraudster then attempted to make a payment through the OLB. It appears that he may have had access to OLB from Miss Z's prior login just before AnyDesk was downloaded. The transaction was blocked by Barclays.

The fraudster then moved to Barclays.Net and initiated the log in procedure, unknown to Miss Z.

At this stage it would be useful to explain that there are two systems through which H could access the accounts and make payments (1) OLB and (2) Barclays.Net.

Barclays say that these are two separate systems with different websites that each require the use of different payment tools. So, they insist that it was not possible for the fraudster to seamlessly move from the OLB platform to Barclays.Net.

What seems to have happened is that when the fraudster initiated the Barclays.Net log-in process, that prompted a message on the smartcard reader with Miss Z asking her to enter the PIN (without specifying the reason for it). Once she did so, another message appeared

on the reader which said “Confirm Log in Barclays.Net. Press OK’. It appears that Miss Z pressed OK to this, which (unknown to her) allowed the fraudster to get into Barclays.Net.

The fraudster then attempted to make payments from Barclays.Net. This started happening at around 3.28pm. The first four payments failed. Barclays say that the first two were abandoned by the fraudster before the payments could be attempted The next two were put through but were blocked by Barclays for a combination of reasons including the size of the payments.

The fraudster then asked Miss Z to delete the Barclays app on her mobile. It was not reinstalled and reactivated until much later in the evening. As a result, she was unaware of what was happening on the account and all she could see was what was showing on her smartcard reader.

The fraudster then moved to another account of H and started making payments from it, for lower amounts. This started at around 3.57pm. They did all the background work necessary to make the payments, such as setting up the new payee etc. All Miss Z could see was a message on her smartcard reader prompting her to enter the PIN for each of the transactions. Miss Z says that the caller told her that she needed to enter the PIN to enable Barclays to refund the fraudulent payments but in reality she was unwittingly enabling the fraudster take money out of the accounts.

Barclays initially told us that each request to enter the PIN was accompanied by a message “Authorise payment reference” but it has subsequently acknowledged that this is incorrect. The accompanying message said “Submit payment reference”. This is important because there is a difference between asking Miss Z to ‘authorise payment reference’ and ‘submit payment reference’. The latter seems to me to carry a weaker connotation that some kind of transactional mandate was being sought or given.

The payments then started happening from that account and soon the entire balance on the account was wiped out. In fact it appears from the bank statement that the account went into overdrawn position.

At that point the fraudster moved back to the main account which had substantial balance and started initiating payments from it, until the balance on that account too was wiped out. Here again, it appears that the account actually went into overdrawn position.

The last transaction out of H’s account happened at 6.21pm. By this point, approximately £1.3 million had been taken out of both the accounts.

Miss Z was on the call with the fraudster during this entire period. However the fraudster had to call her back a couple of times as the calls disconnected. Miss Z says a few calls occurred on her landline as well, due to poor signal on her mobile. She also says that her computer screen was blank during this entrire period.

Towards the end, the fraudster advised Miss Z to re-register Barclays app which she did at about 7pm. Barclays records show that minutes later a new device was registered to the mobile app which didn’t belong to Miss Z. Miss Z says the fraudster had asked her to download AnyDesk on her mobile as well. It is possible that may have given them the access to the registration code sent by Barclays.

The fraudster then gained access to Miss Z’s personal accounts through the app. A payment of £15,000 was made from her personal ISA account to H’s business account. Miss Z says she saw the credit into the business account but she didn’t know that it had come from her

ISA account. The fraudster presented it as part of the refund for the prior fraudulent activities which he said was tackling.

In the concluding call, the fraudster told Miss Z that a full refund would be completed in about five days. When Miss Z asked him to send a notification to her app to confirm this, he disconnected the call.

At 7.22pm, Miss Z emailed her Barclays Relationship Manager. She told him about the calls from Barclays and urged the relationship manager to ensure that the refunds as promised by the bank were made quickly. She was still referring to the fraudster as a member of the Barclays fraud team, though she was beginning to doubt the authenticity of the caller.

Soon after she sent the email, on further reflection, she suspected that she might have been scammed. She then called Barclays fraud team at 8.08pm. An agent said they would block the affected accounts, and advised her to attend her local branch the following morning. No detail was taken about the disputed payments that had occurred. No attempt was made to contact the receiving payment service providers (PSPs) to alert them of the fraud and try and retrieve the funds.

Miss Z and a co-director of H attended a Barclays branch the next morning as advised and explained what had happened. The information from Barclays indicates that despite this the receiving PSPs weren't contacted at least until that evening. However the information we obtained from some receiving PSPs suggest that Barclays contacted them even later.

On 14 December, two payments of £50,000 which had been set up by the fraudster as a '3-day payment' left H's account. They went to one former and one current employee of H. It isn't clear why the fraudster set up these payments to go the employees of H.

Miss Z asked Barclays why the payments went through given that she had already reported the specific transactions as arising from the scam. In response, Barclays said the 3-day payments had a cut off time of 12.30pm on 13 December 2022, after which they could not be stopped. The bank said that the fraud had not been reported to the relevant team until 4.30pm that day and therefore they couldn't prevent the debits. As I understand it, Miss Z was later able to contact the payees and retrieve these two payments.

Miss Z complained to Barclays. She said, in summary:

- All the transactions were unauthorised, and Barclays are liable to reimburse H in accordance with The Payment Service Regulations 2017 (the PSRs).
- Barclays failed to prevent the loss by allowing the payments which were clearly unusual and out of character to normal account activity.
- Barclays' attempts to contact H during the fraud were insufficient. The payments shouldn't have been allowed until contact could be established with her, or (if the bank wasn't able to reach her) the other two signatories, to establish their authenticity.
- Barclays failed to take prompt action on being advised of the fraud. This led to a delay in contacting the receiving PSPs, potentially impacting the total amount ultimately recovered.

Barclays did not uphold the complaint. In summary it said that Miss Z did not take reasonable steps to verify the identity of the caller before providing sensitive account information and access. So they said they won't be able to refund the losses to H.

One of our investigators considered the complaint and recommended that the complaint be upheld. They said, in summary:

1. The payments were not authorised by H. Given the circumstances it could not be said that Miss Z consented to payments being made from the account. At a minimum she did not herself complete the second of the two necessary steps required by the terms and conditions to provide authorisation (she did not follow the instructions to complete the payment, the fraudster did). Therefore, the transactions should be considered unauthorised.

   Further, it is clear that H did not authorise Miss Z to instruct any of these payments to fraudsters. So, any authority she had to give the instructions must have been apparent authority only. However, if the circumstances suggested fraud – as they did here, any reliance on such apparent authority was unreasonable unless Barclays sufficiently investigated whether H had actually authorised the payments. But Barclays failed to do so in any adequate way. Had it carried out proper enquiry, it would more likely have come to light that the payments weren't indeed authorised by H. In the circumstances, the bank couldn't fairly claim that the payments were authorised by H.

   Therefore it would be fair and reasonable for Barclays to refund the payments unless H (or Miss Z) failed with gross negligence to comply with the terms of the account. Taking into account what had happened, it could not be said that H or Miss Z's actions amounted to gross negligence.

2. In any event Barclays failed to take appropriate steps to prevent the losses. If it had acted fairly and reasonably the fraud could have been prevented.

3. In addition, Barclays failed to act fairly and reasonably after Miss Z reported the fraud. In particular it did not act in a timely manner to recover the payments after the fraud was reported. This deprived H of the opportunity to recover more of the funds.

4. Barclays did not handle the matter properly before and after the fraud was reported. The losses meant that H had to make alternative arrangements to ensure that enough funds were available to run the nursing home and arrange a tax deferral with HMRC. All of this caused considerable inconvenience to H.

5. In view of all of the above, in full and final settlement of the complaint Barclays should:
   - Reimburse H all outstanding losses that arose from payments made via Barclays.Net.
   - Pay interest on that figure at the rate of 8% simple per annum from the date of the transactions to the date of settlement.
   - Pay £1,000 to H for the inconvenience caused.

Barclays did not agree. In summary, the bank said:

- A transaction is to be regarded as "authorised" by the customer if the customer (or one of its authorised representatives) uses the payment tools supplied by the bank to signal consent to the payment in question. This is consistent with regulation 67(2) of the PSRs, which provides that consent "must be given in the form, and in accordance with the procedure, agreed between the payer and its payment service provider".

  In this case, this means that the payments will have been authorised if Miss Z, as the authorised representative of the payer (H), invoked the agreed form and procedure for giving consent. There can be no doubt that Miss Z did so, by using the PIN pad reader supplied by Barclays to authorise the payments. So the payments were authorised.

In relation to the alternative reasoning provided by the investigator, the only circumstances capable of putting a bank "on notice" of a fraud such that it must refrain from acting on a payment instruction issued by an agent are circumstances suggestive of dishonesty by the agent that was apparent to the bank. That was simply not the position here. Miss Z was not acting dishonestly. She therefore continued to have actual authority to give instructions on H's behalf. Questions of apparent authority are therefore irrelevant, although Miss Z would obviously have had apparent authority to issue instructions to Barclays as well.

- Even if the payments had been unauthorised, it would not be necessary for the bank to establish that H acted with gross negligence, in order for it not to refund the payments. In the case of 'Larger Corporate customers' like H, the test is simply whether the customer didn't take steps to keep its payment tools secure. H (acting through Miss Z) failed to do so, and therefore the bank isn't obliged to refund the payments under the terms of the accounts.

- The bank could not reasonably have been expected to take any more action than it did, and could not have prevented the losses in the circumstances.

Section B: My provisional decision

I issued a provisional decision, which forms part of this decision and should be read together with this final decision. I partly differed from the investigator in my provisional decision. I said:

The evidence in this case is detailed, which I have read and considered in their entirety. However, I trust that the parties will not take the fact that my findings focus on what I consider to be the central issues, and that they are expressed in less detail, as a discourtesy. The purpose of my decision is not to address every point raised in detail, but to set out my conclusions and reasons for reaching them.

Authorisation and keeping payment tools secure

As noted earlier, the investigator was of the view that H did not authorise the payments. The bank disagreed.

The bank further said that even if the payments were to be regarded as unauthorised, it isn't obliged to refund them under the terms of the account.

I have considered the latter point first as I don't need to resolve the arguments about the former if I agree with the bank on the latter point in any case.

The bank says that under its account terms ('the Terms'), in the circumstances where someone takes an unauthorised payment from its customer's account, the intent or gross negligence as a consideration applies only where the customer is a consumer, a micro-enterprise or a small charity.

The bank says that H isn't a micro-enterprise but a 'Larger Corporate customer', which is defined in the Terms as any business customer which isn't a micro-enterprise, or a charity whose annual income is less than £1 million.

It is not disputed that H doesn't satisfy the criteria to be a micro-enterprise or a charity. So, I agree that H is a 'Larger Corporate customer' as per the above definition in the Terms.

Miss Z submits that H is a small business, and it is wrong to classify H as a 'larger' corporate business customer. I appreciate why Miss Z says so, but here the definition simply means that H is not a micro-enterprise.

Barclays say that in the case of 'Larger Corporate customers', the test of gross negligence is not relevant. The test under the relevant terms for the customer to be eligible for a refund in the event of an unauthorised transaction, is simply whether the customer "didn't take steps to keep [its] payment tools secure" or, alternatively, acted in breach of the Terms.

It says that although the test of "intent or gross negligence" is the default position under regulation 77(3)(b) of the PSRs, the parties may agree to disapply regulation 77 for a customer which is not a consumer, a micro-enterprise or a small charity (regulation 63(5)(b)). The bank says, that is what the Terms do here for 'Larger Corporate customers' such as H.

Miss Z says that there is no confirmation in the Terms that Regulation 77 does not apply.

The relevant section in the Terms say:

*"**If someone takes an unauthorised payment from your account**:*

If someone takes a payment from your account that you didn't authorise, we'll normally refund you as long as you tell us within 13 months of the payment.

However, we won't refund you if:

- *we reasonably think you acted fraudulently (and we may involve the police)*
- *you're a Larger Corporate business customer and you didn't take steps to keep your payment tools secure, or didn't tell us as soon as possible that you had lost your payment tools*
- *you're a Micro-enterprise or Charity and you deliberately or with gross negligence didn't keep your payment tools secure, or didn't tell us as soon as possible that you had lost your payment tools…… "*

I think this has the effect of disapplying Regulation 77, as claimed by Barclays.

So, it seems to me that the test here, under the above terms, is whether H took steps to keep the payment tools secure or didn't tell the bank as soon as possible that they had lost the payment tools.

The fraud was reported as soon as possible. So, the question is whether H didn't take steps to keep the payment tools secure.

Before I consider that - the bank has given an alternative test (for not to refund in the event of unauthorised transaction), which is that the customer acted in breach of the Terms. However, this requirement isn't stated in the above section of Terms.

In this regard, the bank says:

"[H] breached its obligation under regulation 72(1) of the PSRs, namely to use its payment tools 'in accordance with the terms and conditions governing [their] issue and use'. This is by itself sufficient to lead to the conclusion that H 'didn't take steps to keep [its] payment tools secure'…"

Regulation 72 says:

"72.— Obligations of the payment service user in relation to payment instruments and personalised security credentials

(1) A payment service user 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; and

(b) notify the payment service provider in the agreed manner and without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.

(2) Paragraph (1)(a) applies only in relation to terms and conditions that are objective, non-discriminatory and proportionate.

(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."

From the above I see that the requirement to take reasonable steps to keep safe personalised security credentials relating to a payment instrument is separate to the requirement to use the payment instrument in accordance with the terms. So, I don't agree that not fulfilling requirement (1) – even if that was the case here – automatically means not fulfilling (3). And as I said, this requirement wasn't specified in the relevant terms in any case.

Taking all of the above into account, in the event the transactions were unauthorised, I need to consider whether H (or its representatives) didn't take steps to keep the payment tools (personalised security credentials) secure.

The Terms define 'payment tools' as follows:

"What are 'payment tools'?

These are things you use to access your account and make payments that are personal to you. This is how we know we are dealing with you. They can include:

- *"a physical device, like a card*
- *a digital version of a card – in other words, the equivalent of card details but stored electronically on a device such as a computer or mobile; for example, Apple Pay or Contactless Mobile*
- *actions you have to take, which include using passwords, security keys, cards, personal identifier(s), codes (such as Mobile PINsentry) fingerprints, and personal identification numbers (PINs)..."*

The Terms further say that the payment tool itself can be a combination of these, such as card together with entering a PIN.

The mere fact that there was a fraudulent use on the account doesn't automatically mean that the authorised user didn't keep the payment tools secure. This must be considered in the circumstances of each case.

Miss Z says that she did keep the payment tools secure. She says that she did not lose the physical devices and she did not give away the log-in password or PIN to the fraudster.

The Terms do not expand on what is meant by keeping the payment tools secure. Given the phrase's context, this must be a requirement for the customer to take steps to prevent the payment tools being used by a third party to make unauthorised payments.

A key part of this is certainly keeping the physical payment tools safe. But another part of the "payment tools" is "actions you [the customer] have to take", whether alone or in combination with the physical payment tools. So, I think the security of the payment tools includes the protection of those actions against their use by third parties.

For example, if the customer discloses their PIN to a third party, that wouldn't be keeping it secure, even though a PIN is not a physical payment tool. Similarly, if the customer allows third parties to take control of payment tools by directing the customer's use of their PIN, card reader etc, in my view that also would be a failure to keep those tools secure. That is because, even though the physical payment tools may still be safely in the customer's possession, the payment tools that consist of actions are placed under the control of the third party who dictates their use.

In this instance, Miss Z downloaded the AnyDesk software and gave the fraudster access to her computer. This on its own may not have involved use of the payment tools. However, this allowed the fraudster to access the bank accounts through the OLB screen. This he was presumably able to do because Miss Z had logged into OLB just before and it was still open at the time.

The fraudster then attempted to make a payment via OLB. Barclays say that in order to make a payment through OLB, there needs to be an interaction between the OLB screen (which the fraudster had control of) and the Mobile PINsentry or card reader which were with Miss Z. In this instance, it appears that Mobile PINsentry was used. Miss Z says that there was no such interaction.

Barclays say that an eight-digit number displayed on the computer screen had to be input into the PINsentry which in turn would generate a different eight-digit number. This had to be input back on to the computer screen and the 'Confirm' button on the screen had to be pressed to make the payment.

The bank further says that there is a 'Respond' function which is used in PINsentry in this connection, and the evidence provided by Barclays show that the 'respond' function was used at about 15:23, when the OLB payment was attempted.

Therefore, it seems more likely than not that – with the screen blank – the fraudster called out the eight-digit number on the screen to Miss Z who in turn conveyed the eight-digit code generated on PINsentry to the fraudster. However, I am willing to reconsider this depending on any explanation from the parties as to how the fraudster was able to make a payment otherwise.

All that said, no payment occurred through the OLB and as such this action did not cause the subsequent loss.

Once the attempt to make payments via OLB failed, the fraudster moved to Barclays.Net. Here, as I understand it, the following happened:

- On the landing page a warning was displayed which the fraudster confirmed as having read by pressing the 'Confirm' button.

- Once the 'Confirm' button was pressed, he was presented with three ways to login:

Smartcard, biometric and mobile. In this case it appears that the fraudster chose the first.

- A message then appeared on the smartcard reader (which was in the possession of Miss Z) asking her to input the PIN, which she did and pressed OK.

- Then another message appeared on the reader that said "Confirm Log in Barclays.Net. Press OK". Miss Z pressed OK, and this enabled the fraudster log into Barclays.Net.

So, by entering the PIN and confirming log-in, Miss Z followed the directions given to her by the fraudster, even though the directions concerned actions that were a key part of H's payment tools. And that allowed the fraudster to have access to Barclays.Net. I consider that in doing so she did not take steps to keep the payment tools secure. Indeed, by allowing the fraudsters to direct her use of H's PIN and card reader and thereby access H's account, she did the opposite.

And then, subsequently, with the screen still blank, Miss Z put through the PIN several times that allowed the fraudster to make payments out of the account. I regard these PIN entries, both individually and also when taken together with the previous steps by which Miss Z had allowed the fraudster access to the account, as failures to take steps to keep the payment tools secure.

I appreciate that this was a sophisticated scam, and she was deceived by the fraudster. I am aware that she input the PIN in the belief that she was acting on the instructions of a member of staff of the bank and that by doing so she was actually obtaining refunds.

However, as discussed earlier, the test here isn't whether she acted in (gross) negligence. The test is whether or not she took steps to keep the payment tools secure. And for the above reasons I don't think she did so. I consider that her actions allowed the fraudster to access H's account and use the payment tools in a way to make the fraudulent payments.

Therefore, this means that even if the payments were unauthorised (about which I have not made any finding), Barclays isn't obliged to refund the payments for this reason under the Terms because H (or its representative) failed to take steps to keep the payment tools secure.

That said, this finding is confined to refunds the bank is required by legislation to make for payments executed by it without authority, as opposed to other forms of redress arising on a quite different basis.

So, I have also considered whether there are other reasons why it is fair that Barclays reimburses the loss to H, in particular whether there was any error or omission on part of the bank and whether it could have prevented the losses to its customer at any stage during the fraud. I have considered this in Section B below.

Did the bank do enough to prevent the fraud?

H also argues that in any case Barclays failed to prevent the loss by allowing the payments which were clearly unusual and out of character to normal account activity. H's complaint in this regard is as below:

- When the fraud was ongoing, the bank detected some unusual activity and made an unsuccessful attempt to contact Miss Z on her mobile. But it made no attempt to contact H on their landline number or contact the other two cardholders.
- Despite being alerted to unusual activity, the bank failed to monitor the account for

highly suspicious activities and permitted unusual transactions to leave the account in 'devastatingly' large sums. What happened to the accounts was 'unprecedented'. The volume and value of the transactions were highly unusual. The account history will highlight that H had never made transactions of these values, these volumes and had never gone into overdrawn position.

- Had Barclays taken more steps to ensure they had spoken to a cardholder, or put the account on hold until it had, this would have stopped the fraud from being successful. The payments shouldn't have been allowed until contact could be established with her, or the two other account holders (if the bank wasn't able to reach her), to establish their authenticity.
- Regulated firms like Barclays are required to conduct their business with due skill, care and diligence and to 'pay due regard to the interests of its customers. Firms should also have taken proactive steps to look to identify and help prevent transactions particularly unusual or out of character transactions that could involve fraud or be the result of a scam (something also recognised by the British Standards Institute's October 2017 'Protecting Customers from Financial harm as a result of fraud or financial abuse – Code of Practice'). This means that, particularly with the increase of sophisticated fraud and scams in recent years, there are circumstances where a bank should fairly and reasonably take additional steps, or make additional checks, before processing a payment, or in some cases decline to make a payment altogether, to help protect customers from the possibility of financial harm.
- Regarding the recoveries of funds, the incident was reported to the fraud team around 30 minutes after the incident. The person on the phone did not take any action and advised Miss Z to report to the local branch the next day. There was no plan for recoveries until two days after the fraud. Had the bank taken immediate steps to recover the funds, it would have been able to recover more than it did.
- Further, two payments of £50,000 each were sent despite Miss Z reporting the fraud well within the recall time. H did not get back these payments until over a month afterwards which placed additional strain on the business, and in fact it was H which managed to get back the sum from their employees and not the bank.

The relevant terms and conditions in this case conferred on Barclays rights (but not obligation) to:

1. Refuse any payment instruction if it reasonably suspects it is connected to a fraud, scam or any other criminal act. And this includes where it reasonably thinks the funds are being obtained (from its customer) through deception.

2. Delay payments while fraud prevention checks take place and

3. In such circumstances contact the customer as quickly as possible to tell them that it hasn't followed the instruction and explain why.

Those terms must be read against caselaw, namely the Supreme Court's decision in *Philipp v Barclays Bank UK PLC [2023] UKSC 25* which establishes that:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, the bank must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.

- The express terms of the current account contract may modify or alter that position. For example, in *Philipp*, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP

fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a duty to do so.

So, the starting position at law is that:

- Barclays was under an implied duty at law to make payments promptly.
- It had a contractual right not to make payments where it suspected fraud.
- It had a contractual right to delay payments to make enquiries where it suspected fraud.
- It could therefore refuse payments, or make enquiries, where it suspected fraud, but it was not under a contractual duty to do either of those things.

Whilst the current account terms did not oblige Barclays to make fraud checks, I do not consider any of these things (including the implied basic legal duty to make payments promptly) precluded the bank from making fraud checks before making a payment.

And whilst Barclays was not required or obliged under the contract to make checks, I am satisfied that, taking into account longstanding regulatory expectations and requirements, and what I consider to have been good practice at the time, it should *fairly and reasonably* have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

Indeed, I see on Barclays' business banking website, the below is prominently stated as one of the things the bank does to help the businesses:

"*24-hour fraud protection*
Keep your finances safe – we look out for you and your money around the clock"

In reaching my conclusions about what Barclays ought fairly and reasonably to have done, I am mindful that:

- FCA regulated banks are required to conduct their "business with due skill, care and diligence" (FCA Principle for Businesses 2) and to "pay due regard to the interests of its customers" (Principle 6).

- Banks have a longstanding regulatory duty "*to take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime*" (SYSC 3.2.6R of the Financial Conduct Authority Handbook)

- Over the years, the FSA and its successor the FCA have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by banks to counter financial crime, including various iterations of the "Financial crime: a guide for firms".

- Regulated banks are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. These requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage risk, e.g. through customer due-diligence measures and the ongoing monitoring of the business relationship including through the scrutiny of transactions undertaken throughout the course of the relationship.

- The October 2017, BSI Code, which a number of banks and trade associations were

involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code, but in my view the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now.

- Barclays is also a signatory of the CRM Code. This sets out both standards for firms and situations where signatory firms will reimburse consumers. The CRM Code does not cover all authorised push payments (APP) in every set of circumstances (and it does not apply to the circumstances of these payments), but I consider the standards for firms around the identification of transactions presenting additional scam risks and the provision of effective warnings to consumers when that is the case, represent a fair articulation of what I consider to be good industry practice generally for payment service providers carrying out any APP transactions.

Overall, taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Barclays should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.

- 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). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.

- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – as in practice all banks do.

- Have been mindful of – among other things – common scam scenarios, the evolving fraud landscape (including for example the use of multi-stage fraud by scammers) and the different risks these can present to consumers, when deciding whether to intervene.

As a matter of fact, in this case, as noted below, Barclays did try to take some actions as it was suspicious of the account activities. So, the question for me is whether that was enough or whether it could have fairly and reasonably done more, and had it done so whether that would have prevented the losses to H.

I have considered below what had happened here:

- Barclays declined a payment of £12.99 at Domino's Pizza. The bank says that it was also suspicious about a payment of £5.99 (also to Domino's Pizza) and £60.85 to another company. It is unclear what made the bank decline the first of these and be suspicious about the other payments. However, it seems that this would have been the first indication to the bank of some suspicious activity on the account.

- The bank then sent a text at 12.06pm about this. The text message said: "*Hi, we need to confirm some recent spend on your debit card ending XXXX. Please reply to messages from 80167. Before you do, STOP & THINK SCAM. Genuine organisations*

will never call you, to say what answers you should send for these fraud checks, if you've had such a call, it might be a scam. "

The bank then sent another message at 12:10pm which said "*£12.99 at DOMINO'S PIZZA was DECLINED, £5.99 at DOMINO'S PIZZA, £60.85 at [*other company name*]. If you made all the payments above please reply Y, if there are any that you didn't make please reply N*. "

The bank didn't receive any response to these two text messages. This was because at 12:06 Miss Z received the first call from the fraudster (pretending to be Barclays) and he was already in discussion with Miss Z about the suspicious activities.

- The bank says that having received no response to the texts, it called Miss Z at 12.25pm to discuss the account activity. The above two text messages and this call appear to be from its automated system.

  The bank says that she did not answer. Miss Z says that she was busy at work, and in fact that was why she had asked the earlier caller to call back later. I can't see that the bank left any voicemail or sent a further text message at this time.

  So, the situation at this time was that the bank was suspicious of some transactions on the account, attempted to ascertain from one of the signatories on the account whether the transactions were genuine, firstly via two texts and then by a phone call, but did not get any response.

- The bank says it tried to call Miss Z again at 2.34pm but the call was disconnected. However, I see that the investigator has subsequently established that the bank couldn't be sure that Miss Z actively declined the call. It appears that this too was a system generated call, which tried to call her and connect her to an agent. The bank has acknowledged that there may have been a connection error which meant that the connection would have been cut off even before the call was attended by Miss Z.

  I consider it reasonable to expect that if there was a connection error and therefore the call wasn't connected, the bank should have attempted to call Miss Z again. But there is no evidence that it did.

- As the bank wasn't able to talk to her, it went ahead and blocked the card. This suggests to me that it had sufficient concerns about the activities on the account and the lack of response from Miss Z, for it to have taken this step.

  This to me seems a reasonable response to what had happened thus far.

- The bank then sent a text message at 2.36pm that it had temporarily stopped the card to protect H against fraud, and asked Miss Z to contact the bank. Unfortunately, I think that this message reinforced Miss Z's belief that she was in fact talking to the bank earlier in the day and that the bank's staff were following their assurance to help her. She says that she didn't call the bank as she was expecting a call from the 'bank' soon anyway.

- After the text message at 2.36pm, the next alert to the bank would have been when the fraudster attempted to make a payment out of the account through OLB.

  This happened at about 3.23pm. The fraudster attempted to make a payment of £9,898.78. The bank says this was picked up by its OLB fraud transaction monitoring

system because '*it was a large payment being sent to a new beneficiary* …'

The bank says that the payment was flagged and placed in a queue to be checked by the Fraud team. It says that the payment was 'delayed' until such time a member of the Fraud team could verify it with H.

The internet history provided by Miss Z suggests that at that point the OLB access was in fact suspended. The relevant web page at 15:23 stated "https://www.barclays.co.uk/goto/pfs-olb-accountsuspended".

This suggests that the account (or the OLB access at least) was suspended rather than just the payment being delayed. Nevertheless, the fact remains that the payment was flagged as suspicious and therefore the bank was alerted to it.

- By this point the bank was also alerted to the remote access, which had happened by then.

  In addition, between this point and before a member of the Fraud team attempted to call Miss Z (see below), the fraudster had moved over from the OLB system to the Barclays.Net system and attempted two unusually large payments for £55,676.78 and £50,000 from the account, which did not go through. The bank says that they were 'deleted' by the fraudster, but this information would have been available to the bank at this time.

- It is good to note that the Fraud team attempted to call Miss Z about the OLB payment at around 3.40pm but as she was on the call with the fraudster, they couldn't reach her. So, they left a voicemail asking her to get in touch.

  Firstly, in my view the voicemail left by the staff wasn't very helpful. The staff simply said that they were calling about 'the payment on your account' and as they were unable to get in touch, requested Miss Z to call back.

  Had Miss Z listened to the voicemail she could have very well thought that this was in relation to the debit card payments. Further there was no urgency about the call nor did the staff ask her to contact as soon as possible.

  The bank says that it was at this point (at about 3.42pm), because the staff was unable to contact Miss Z to verify the payment, they cancelled the OLB payment and suspended the access to OLB.

  If so, I consider that Barclays ought to have done more here and blocked access to Barclays.Net as well.

  I say this because there was a manual intervention here by the bank's Fraud team, who ought to be well versed in identifying suspicious activities on the account and taking appropriate steps to help its customer. So, when the staff picked up the alert and attempted to call Miss Z, they would have seen or ought to have seen the following:

  1. There were suspicious card transactions earlier in the day which eventually led to the bank not only declining the transactions but also blocking the card.
  2. Then a payment happened on OLB about which the bank was sufficiently concerned to block it and attempt to check with one of the customer's signatories whether it was they who were making the payment.
  3. There was a remote access on the account starting just before this payment was attempted and which was still ongoing when the staff attempted to call Miss Z.

4. As soon as the payment was blocked but before the staff called Miss Z, someone moved over from OLB system to Barclays.Net system and attempted two unusually large payments for £55,676.78 and £50,000 from the account, which did not go through. The associated error message stated that the payments did not go through because the beneficiary bank had confirmed that the beneficiary account details 'did not exist'. And the beneficiary bank here was in fact Barclays.
5. The staff tried to contact Miss Z, but she was on a call and not contactable. This, in combination with the remote access and suspicious activities on the account immediately after the remote access ought to have alerted the Fraud Department staff about the possibility of a fraud ongoing by takeover of the computer.

So, I consider that extending the block which had been applied to OLB to Barclays.Net until Miss Z or one of the account signatories could be contacted would have been a reasonable action in the circumstances.

Had that block happened, I consider it more likely that the losses to H could have been prevented. Firstly, all the fraudulent transactions happened after this point. So, any such block would have prevented the fraudster from proceeding further. Secondly when a block is in place, the bank would usually want to be fully satisfied that the transactions are genuine before removing the block and here that would have involved talking to Miss Z (or other signatories to the account). That in turn would have highlighted the fraud attempt. As such I consider the bank missed a good opportunity, perhaps for the first time, to prevent the fraud and financial loss to H.

- Moving on, soon after the attempted call by the bank, the fraudster tried two more payments of £53,291.78 (at 3.48pm) and £5,000 (at 3.50pm). These payments were blocked by the bank.

  Barclays says that they were blocked for one or more of the following reasons: high value, a round figure and a second payment being attempted soon after the first and to the same payee.

  The bank says that the payments were held for additional security checks whereby a member of its Fraud team needed to call Miss Z to confirm if the payments were genuine. However, there is no evidence that the bank attempted to contact Miss Z or any other signatory until 6.13pm by which time most of the funds have left the account.

  I consider this was another missed opportunity because even by that time no payment had gone out of either of H's accounts.

- An internal email within Barclays was sent minutes later at about 3.49pm. The subject line was 'Biocatch suspected HIGH RISK session'. The email shows that there were in fact two remote access alerts (one alert as soon as the fraudster had the remote access at about 3.25pm and another one at 3.49pm which may have triggered this email).

  The email also referenced the two payments made at 3.33pm and 3.48pm respectively, which had been rejected.

  Barclays says that the email highlighted that potential remote access had been detected in respect to these payments but says this didn't warrant a suspension because a high proportion of business customers use remote access while using Barclays.Net.

  However, in my view this needs to be considered in the context of H's accounts and the

normal activity on those accounts. The bank has provided no evidence that H routinely tended to use remote access (or at all) in the past to operate the accounts via Barclays.Net. Secondly, a lot of suspicious activities had already occurred around this remote access and that is something the bank ought to have taken into account here.

The bank has later admitted that the Fraud team should have called Miss Z to query the log-in from a different location, though it said that its 'standard practice' is that it ought to have called Miss Z within three hours.

I have not been provided any documentation to show that the 'standard practice' of the bank is to call within three hours. Nevertheless, in this case, given all the previous flags, it is reasonable to expect that the bank ought to have acted sooner.

In fact, in another case, when asked to explain the Biocatch system, the bank told us this:

".. *It is a profiling system that records the user's interactions*….. *and used to access if any third party access is gained*. *Should the interaction be different* (to previous usage) ... (and if the risk score is above a certain level) *...* that *would be deemed as suspicious and may be flagged / deferred* ….. *requiring contact with our customer or safeguards being applied preventing the use of this payment method*. "

Given that the Biocatch alert was 'suspected HIGH RISK session' I consider the above ought to have happened. The bank ought to have contacted the customer, failing which taken safeguards to prevent the use of the relevant payment method, which in this case was Barclays.Net.

Incidentally, the bank never called within the three hours in any case. It says that it made the relevant call only the next day, despite the alert.

The bank says that even if it had called Miss Z, she wouldn't have answered the call. But had it called Miss Z and if she wasn't available, it could have extended the block which had already been applied to OLB to Barclays.Net until Miss Z could be contacted. It would have been a reasonable action in the circumstances. Had that happened, the bank would have prevented any loss occurring from H's accounts because even at this time no payment had gone out of the accounts. Also, it could have attempted to contact the other signatories to the account, but it failed to do so until much later.

Overall, I consider this was yet another opportunity missed by the bank to prevent the loss to H.

- It appears that because the two payments were blocked under the (main) account, the fraudster moved to another account of H and started making payments from it. And in about 40 minutes or so the fraudster made several payments out of the account which wiped out all the money on the account and put it in an overdrawn position. From what I can see three of those payments were 'rejected' and subsequently re-credited to the account and only because of that, the end of day balance was about £2,000 in credit.

  From the historical bank statements provided by the bank I see that this level of activity was highly unusual to the account. I see that this is an interest bearing 'premium account' which Barclays' website describes as an easy access deposit account. In the preceding six months there was not a single payment out of the account. Then all of a sudden, several payments were made out of the account all to new payees. And within a short time almost the entire balance was wiped out.

In fact, it appears that the fraudster continued to try and take more payments out of the account despite a very low / nil balance. I can see that they attempted four bulk payments totalling about £240,000 which were 'deleted' due to insufficient funds. They then attempted one more bulk payment for about £15,000 which was 'stopped'.

All of this happened on the back of all the 'red flags' I have discussed earlier. Yet there was no intervention from Barclays at all when all of this happened.

I think that had Barclays intervened to check what was going on, it would have been concerned about the account activity and more likely blocked Barclays.Net pending contact with H. But unfortunately, that did not happen and so this was yet another opportunity missed by the bank.

- Having exhausted the account balance on this account, the fraudster moved back to the main account where the first two transactions had already been blocked. After returning to the main account, the fraudster started swiftly transferring money out of it.

  From what I can see, the fraudster made 16 bulk payments to 62 payees (most of them new payees – with the rest being new payees set up just earlier under the other account), and two single direct payments. In addition, I can see at least four payments which the bank appears to have withheld.

  In just over an hour, the balance on the account dropped from about £1.2m to an overdrawn position.

  In his view the investigator said that these payments were out of character to normal account activities. In response the bank listed the usage on the account for the preceding six months, especially in relation to Barclays.Net and said that "*None of this (the payments) is unusual when considered against [H's] general business activity, its use of B.Net to make regular high-value bulk payments, or when considering the use and purpose of B.Net for business and corporate customers generally*."

  I have already said that in my view, the bank had to consider whether its customer was at risk of fraud by considering the activity in relation to the specific account in question, irrespective of which system was used.

  So, I have reviewed the account activity for the prior six months. From what I can see, the average daily spend on the account was no more than £10,000 including *all* forms of payments and typically 1% to 3% of the available balance.

  There were of course days when the payments were in excess of this average figure. However, the highest single payment on the account on such days was for about £100,000, which happened six months earlier. But even on that day, the maximum spend was only about 10% of the available balance.

  Compared to this, the total payment here was about £1.2m and 100% of the available balance was paid out, in just about an hour. And it followed immediately upon the emptying of the deposit account and the failed bulk payments from it, which I've described.

  Further, during the period of previous six months, there were 24 transactions from Barclays.Net – so an average of four transactions per month. Of these, there were only 14 occasions when a bulk payment was made, so roughly twice a month. I also see that there was a pattern to the bulk payments in the sense that H typically made two

bulk payments at the end of each month - one for the payment of wages and the other for invoice payments. Compared to this, here there were 16 bulk payments on a single day outside of the normal pattern.

In addition, the bank has said that in total there were 18 new payees during this period, so an average of three new payees a month but here there were a large number of new payees on a single day.

Given all this, I don't think it is reasonable at all to say that the activity on the account that day was not unusual. It was clearly highly unusual.

In addition, I previously mentioned that the very first two payments on Barclays.Net were blocked due to combination of high value, round figure and/or another payment to the same payee attempted soon after the earlier. Subsequently, there were multiple times when payments were made with the same issues but yet on those occasions the bank did nothing.

For example, five payments were made to the same payee within six minutes. In another instance, seven payments were made to another payee within 15 minutes. This is compared to the bank's concern earlier that two payments in quick succession were made to the same payee – which contributed to the bank blocking that transaction.

Overall, I consider that there were multiple points during this one-hour period when the bank could have intervened, but it failed to do so.

- Ultimately, in about 2½ hours, over 90 payments were made to 62 new payees at multiple PSPs. Over a million pounds had been debited from H's accounts, completely wiping out the entire balance on both H's accounts putting them in overdrawn position. Large multiple payments of identical amounts were being made out of the account in quick succession. The payments were completely out of character to normal account activities. And yet the bank failed to make any effective intervention.

- Barclays did attempt again to call Miss Z at 6.13pm. It was rather late in the sense that by that time almost all of the funds had already been transferred out. The bank couldn't contact Miss Z as she was still on the phone with the fraudster. So, it emailed Miss Z and another signatory.

  Miss Z says that the email to her was sent to her personal email which wasn't monitored and not to her company email.

  Nevertheless, the other signatory also got the email, but the email just said: "*Please be advised that we would like to speak to you with regards to a recent query. Please could you call back your earliest convenience* …"

  In my view this was vague and showed no urgency to the recipient to prompt them to call immediately.

  A further £100,000 went from H's account after this.

- Soon after the call with fraudster ended, Miss Z emailed H's relationship manager (at about 7.20pm) enquiring when the refunds would be received as promised by the bank (as she was still under the impression that she had been speaking to a bank staff). She didn't get a response, which given the time of the day was understandable.

  She was then worried about what had happened and suspected fraud. So, she called

Barclays to report what had happened, and spoke to a staff member of 'Fraud Experts team'.

I have listened to the call. It is clear from the call that Miss Z was very distressed and was reporting a big fraud on the company. She told the staff member that no money was left on the account to even buy food or supplies for the care home.

Yet the staff member didn't take any detail about the transactions that had occurred on H's accounts, did not attempt to recall the funds from the receiving PSPs but simply advised Miss Z to go to a branch the following day and report what had happened.

Once again at this stage I don't think the bank acted fairly and reasonably. As I said, the bank's customer had reported a fraud on their account. The amount involved was very large and the bank (especially the 'Fraud Experts team') knew or ought to have known that fraudsters move money quickly and so it was important to act swiftly to try and recover as much as possible. Instead, Miss Z was advised to go to a branch the next day, thereby losing valuable time.

Barclays told us that when Miss Z called to report the fraud, at no point did she mention to the fraud expert about Barclays. Net, whereas she was aware that OLB and Barclays.Net were completely different platforms and so she should have called Barclays.Net helpline.

So, it basically suggests that it was her fault that she called the 'wrong' helpline. The bank also says that "*Barclays' usual procedure, which is entirely reasonable and industry-wide practice, is to attempt to recover funds within 24 hours of being notified of a scam, which is what happened here*"

I do not consider this to be a fair and reasonable position. Miss Z is not the expert here; it is the bank. Indeed, she called the 'Fraud Experts' team. So as 'experts' they ought to know what to do. The bank may have chosen, for its own reasons, to operate separate helplines in relation to its OLB and Barclays.net systems, even though customers could use both or either, to access the same account. Ultimately, the money went from the same bank account, and their customer had reported fraud and loss of a very large sum of money from that account. So, it was for the bank to take necessary action. The bank's customer had just lost over £1.3m and for the bank to say that it had 24 hours to take any recovery action is unreasonable.

I consider that the bank missed yet another opportunity here to try and prevent at least some losses to its customer. I am of the view that the bank ought to have taken steps to contact the recipients' PSPs swiftly when Miss Z reported the fraud to it on 12 December evening.

When the investigator put this to Barclays, it said that it was unable to obtain details as to when all of the funds were dissipated from the various beneficiary accounts. So it couldn't say whether even if it had contacted the receiving PSPs immediately that would have made a difference.

On my request, the investigator contacted the other PSPs to get a clearer picture of what had happened. Given the large number of transactions to various payees across multiple PSPs it has been difficult to get a full picture.

However, the information we have received does indicate that the fraudsters were able to move funds swiftly out of the recipients' accounts. So, to that extent I agree with Barclays that a sizeable proportion may have already been transferred out of the

recipients' accounts even if Barclays had acted quickly on being advised of the fraud.

- Miss Z went to the branch the next day with another director at around 11am and reported what had happened. Even after that the bank made no attempt to contact the PSPs to where the money had gone. The bank told us that it did not start contacting the receiving PSPs until around 9pm that day. But some of the information we received from other PSPs contradicts this too in that they say they received notification from Barclays later than the 9pm quoted by the bank.

- During Miss Z's initial call with the bank on 12 December, the staff member told her that he had blocked all the accounts to prevent further payments going out. Yet, two payments of £50,000 went out two days after the scam was reported, though they went to H's current and past employees and were subsequently recovered by Miss Z.

  The bank says that the 3-day payments had a cut off time of 12.30pm on 13 December 2022, after which they could not be stopped. It says that that the fraud had not been reported to the relevant team until 4.30pm that day and so they couldn't prevent the debits. This appears to be another internal failure on part of the bank.

Taking all of the above into account, I find that at several points the bank failed to act as I consider it should and that, if it had done so, H would not have suffered any of its losses, as the accounts would have been blocked before any of the fraudulent payments were made; and that from an early stage thereafter, during the course of the fraudulent payments, it repeatedly missed further opportunities to intervene which would have prevented the subsequent payments from being made.

So, I intend to uphold H's complaint against it.

Should H accept some responsibility for the loss?

I have then considered whether H should accept some responsibility for the loss due to any contributory negligence on its part or on the part of its representative acting on its behalf.

To start with, in my view this was a sophisticated fraud in the sense that the fraudster was cunningly able to interpolate what he said to Miss Z with genuine actions from Barclays.

For example, he was able to call out some suspicious payments at least one of which Miss Z could see on the statement. The call was timed in such a way that it coincided with a genuine text from the bank about this issue. After she advised that she did not make those payments, he said he would take care of it, and then soon after she got a genuine text from Barclays that the card had been blocked. In addition, the fraudster was able to provide details of genuine transactions which happened earlier in the day and provide details of the names of H's staff and their wages.

Considering what had happened, it seems quite possible to me that the fraudsters may have deliberately triggered a set of actions which they could then use, to convince Miss Z that they were indeed calling from the bank.

So, I can see why Miss Z was convinced that she was talking to the bank. Then in the second call the fraudster created a sense of urgency by advising her that several fraudulent transactions had happened since the first call.

Therefore, the starting point to me is that Miss Z's actions should be considered in the light of this. However, there are other factors which also need to be considered:

- The bank has said that it had provided warnings and information that raised awareness of latest scams and how to protect one's business from becoming a victim.

  Most of what Barclays has indicated, happened over three years ago, and some as far back as 2017. So, I can't say that these warnings were timely. Miss Z did not have sight of any of the bank's in-transaction warnings relevant to this type of scam when the transactions took place. This is because her computer screen was blank throughout the time the fraudster made the payments. Therefore, the warnings would have only been visible to the fraudster and so it cannot be that Miss Z actively ignored the warning.

  That said, I acknowledge that some warnings had been given to H / Miss Z in the past about frauds and scams and downloading software.

  For example, though Miss Z did not log into Barclays.net on this occasion, she had done so on earlier occasions. And when she did so, she would have noticed (at least from August 2022 onwards) a fraud warning that fraudsters continue to call customers impersonating Barclays in order to trick them into giving access to the computer or gain security codes to make payments, and that the bank would never take control of the computer to carry out updates or upgrade to a new portal or ask customers to download from any site other than from Barclays.

- During the second call, the fraudster persuaded Miss Z to download the AnyDesk software. Miss Z says that the caller told her that this was anti-virus software and needed to be downloaded to check whether her computer had been infected.

  Once AnyDesk was downloaded, my understanding is that she would have to call out a code shown on her computer screen to the caller which they need to input at their end in order to enable them access her computer.

  If that was the case, I consider that she would have known or ought to have known that she had given access to her computer to someone else, though I accept that at that point in time she would have thought that she was following the instructions given by its bank and was giving access to a member of bank staff.

- Having obtained the access to the computer, the fraudster attempted to make a payment from OLB. I have already mentioned why it seems more likely that Miss Z may have given the eight-digit code on the mobile PINsentry reader to the fraudster that enabled them to initiate the OLB payment. However, this action did not cause the subsequent loss.

- After unsuccessfully attempting to make transfers via OLB, the fraudster moved to Barclays.Net and initiated the log in procedure, unknown to Miss Z. I have already noted that Miss Z input the PIN and pressed OK to confirm log-in.

  When this was put to Miss Z, she said that she did not actively ignore this message. She said at that time she was distracted by the fraudster who asked her to report the fraud on the Action Fraud website whilst the bank was in the process of refunding the payments. She says that was why she hadn't quite cottoned on to the log-in activity at the time.

In support of this she has given us a screenshot from her mobile phone which shows that there was a google search for 'action fraud' on her mobile at around that time. It doesn't show that she was reporting at that time the initial fraudulent transaction to Action Fraud by entering data on their website and I've seen nothing to that effect.

Nevertheless, I accept that she may have been checking Action Fraud website around that time and it is likely that she was distracted as she says.

- After this, the payments started. All Miss Z could see was a blank screen and repeated instructions on her smartcard reader to enter the PIN, and then to enter OK to the 'payment reference' shown on the reader.

  Barclays has said that Miss Z knew H could only use Barclays.Net to authorise payments, not to seek refunds. The suggestion here is that she couldn't have been inputting the PIN on the belief that H was receiving refunds.

  However, nowhere in the documentation provided by the bank is it stated that a refund wouldn't be given this way. Clearly Miss Z thought H was receiving refunds into the account. And as noted by the investigator this was a unique situation and there is no evidence Miss Z had encountered a similar situation before.

  So, it is fair to say that she wasn't to know that refunds on situations like this cannot be obtained this way. As stated earlier, she genuinely thought that she was talking to the experts here (the bank) and was following their instructions.

- However, it is the case that she saw these messages and input her PIN for about 32 times. This went on for nearly three hours with her screen blank during all this period.

  Whilst I can understand her action to start with, as the time went on and as she kept inputting the PIN with no indication of how that repeated action was achieving what the fraudster promised her, I think it is reasonable to expect that she should have started reflecting on what was going on and taken steps to verify whether what the caller said was true. And if she couldn't verify (because the screen was blank and she had no access to the app) then not to proceed further until the caller's story was confirmed otherwise.

  It also wasn't the case that she was on the same call during this entire period and so had no break. It appears that there were multiple calls from the fraudster during this time, some to her mobile and some to her landline. It may be that the calls happened in quick succession, but I do think that the breaks in the call would have given some time to allow her to reflect.

  So, I consider that after a certain point when she kept repeatedly inputting the PIN, there was a lack of care that went beyond what a reasonable person in that position would have shown.

As I said, this was a sophisticated fraud and Miss Z was under pressure to try and recover the fraudulent payments. So, her actions to start with are understandable. It was only as time went on and as she kept repeatedly inputting the PIN several times without knowing what was happening, I consider that at some point during that period she could have taken some steps. As time passed and more transactions were made, Miss Z's continued conduct in entering the PIN became increasingly unjustifiable.

It is difficult to precisely identify the exact point in time when that should have happened. However, given the persuasive nature of the fraud, it is reasonable to conclude that this

would have happened later during the fraud rather than earlier, by which time some transactions would have already gone through for which I don't think H should be held responsible.

I also consider that – for all the reasons I have already explained – the extent of error or omission on the part of Barclays was much higher than that of H. Further, as explained, Barclays was in a better position to detect and prevent the fraud. So, it is fair that any apportionment reflects this.

In cases like this, how the apportionment of the losses should be made is not an exact science. But after weighing up everything, I consider it fair to conclude that H bears 25% of the loss with the rest borne by Barclays.

Inconvenience caused to H

I agree that this matter caused considerable inconvenience to H for the reasons given by the investigator. This included:

- The Bank not taking appropriate steps in the first place when informed of the fraud but asking the directors to visit the branch.
- Making the two 3-day payments despite being told of the scam well in time. This meant that H had to take steps to try and recover them from their existing employee and the ex-employee. This also would have caused a loss of reputation.
- The losses meant that H had to make alternative arrangements (I understand by way of loan from the directors and family members) to ensure that enough funds were available to run the business.
- H also had to engage with HMRC to enter into a tax deferral arrangement.
- I also see that H (the director) had to spend considerable amount of time afterwards trying to reconcile with the bank all the outgoing payments with various recoveries to try and understand what the impact was.

The investigator recommended that Barclays should pay H £1,000 for the inconvenience this matter has caused, which I consider fair and reasonable in all the circumstances of this complaint.

Summary of my findings

1. Even if the payments were unauthorised (about which I have not made a finding), Barclays isn't obliged to refund the payments for this reason under the Terms because H (or its representative) failed to take steps to keep the payment tools secure. However, there could be other reasons why it is fair that Barclays reimburses the loss to H.

2. It is my view that the bank missed multiple opportunities to prevent the loss to H. So, I consider it fair and reasonable that it should compensate H for it.

3. However, I also consider that there was some contributory negligence on the part of H. Therefore, it is fair to allow for this in deciding the fair compensation. I consider it fair to conclude that H bears 25% of the loss with the rest borne by Barclays.

4. This matter caused considerable inconvenience to H. So, it is fair that Barclays compensates H for it.

Fair compensation

The fair compensation should be calculated as set out below:

1. Arrive at 75% of the loss under each account. The loss figure is the sum of disputed payments made from each of the two accounts less the sum recovered to date under each account.

2. In relation to the loss incurred on the business current account (account ending *064) calculate interest on the loss at 8% simple p.a. from the date of payments to the date of settlement.

   I consider this is fair because though the account earned little interest, the relevant question is the opportunity cost of the lost funds to H. In this case, I cannot be certain about the cost to H of being deprived of the money because it might have used the funds in a variety of ways. It is however clear to see that this was a large sum of money, and the loss has had a big impact on the company's finances. In the circumstances, without any compelling reason to depart from our usual approach, I consider it fair and reasonable that Barclays pays H simple interest at 8% p.a.

3. In relation to the loss incurred on the interest-bearing premium account (account ending *281), as I noted previously, there was hardly any movement on the account prior to the fraud. So, I consider it reasonable to assume that the money lost on the account would otherwise have remained in the same account. So, it is fair that Barclays pays interest on the loss under this account at the rate it would have earned had the money remained in the account.

4. £1,000 for the inconvenience this matter has caused.

5. Miss Z believes that Barclays should also pay her interest on the two £50,000 payments that went out of the account after the she advised the bank of the fraud. She says that the payments shouldn't have happened in the first place, and then it took more than a month for the sum to be recovered.

   This refers to the '3-day' payments that went on 13 December 2022, after Miss Z advised the bank of the fraud on 12 December and again that morning. As noted earlier, the bank has told us that the fraud had not been reported to the relevant team until 4.30pm that day and so they couldn't prevent the debits.

   I have already noted that these two payments shouldn't have gone out in the first instance as the bank was already put on notice of the fraud. So I agree that it is fair that the bank pays her interest on these sums from the date of the payments to the date of recovery. Interest should be paid at 8% simple p.a.

6. So, the fair compensation is (1) + (2) + (3) + (4) + (5). But please also see below my award limit.

My provisional decision

Where I uphold a complaint, I can award fair compensation requiring a financial business to pay compensation of up to £375,000, plus any interest and/or costs that I consider appropriate. If I consider that fair compensation is more than £375,000, I may recommend that the business pays the balance.

Determination and award: I uphold the complaint. I consider that fair compensation for the financial loss should be calculated as set out above. My provisional decision is that Barclays Bank UK Plc should pay the amount produced by that calculation up to the

maximum of £375,000 (including distress or inconvenience).

It should also pay interest on £375,000 at 8% simple p.a. Given that most of the loss has arisen from the current account, I consider it fair that Barclays pay interest at this rate on the £375,000. Interest should be paid from 12 December 2022 to the date of settlement.

Recommendation: As the amount produced by the calculation of fair compensation as set out in the earlier section is more than £375,000, I recommend that Barclays Bank UK Plc pays H the balance together with balance interest."

Section C: Responses to my Provisional Decision

Miss Z acting on behalf of H said that H largely agrees with the Provisional Decision but does not consider it fair that the company should bear 25% of the loss.

Barclays said it has nothing further to add. It has however confirmed that based on the current Provisional Decision, it would pay the recommended amount above the award limit.

Section D: 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, I see no reason to depart from the conclusions I reached in my Provisional Decision. I remain of the view that the settlement set out in the Provisional Decision represents a fair and reasonable outcome to this complaint.

I will however address the points raised by Miss Z in response to the Provisional Decision.

- One of my provisional findings was that, in relation to the blocked OLB payment, it was more likely than not that Miss Z revealed the eight-digit number generated on the PINsentry to the fraudster. I did however say that I am willing to review this in the light of any further submission from the parties.

  In response, Miss Z insists that she did not share any code with the fraudster and the PinSentry device was not used at any time. She believes that the fraudster was not able to make the payment via OLB because they did not have the (right) code.

  This is not borne by the available evidence, as I have explained in the Provisional Decision. Nevertheless, I sought clarification from Barclays whether it is possible that the payment was blocked because the fraudster did not have the (right) code.

  The bank has said that if the fraudster entered the code incorrectly, that would have prevented them from progressing the payment and therefore no payment would be made. And such attempts / failed payments would not make their way to its fraud department. On this occasion the payment in question was successfully completed (i.e., the correct eight-digit code was provided) as it was on the point of leaving H's account and the only reason it didn't was because it hit the bank's fraud triggers.

  Having reviewed all the submissions again, I remain of the view that it is more likely than not that – with the screen blank – the fraudster called out the eight-digit number on the screen to Miss Z who in turn conveyed the eight-digit code generated on PINsentry to

the fraudster. That said, no payment occurred through the OLB and as such this action did not cause the subsequent loss.

- Miss Z says that I have not properly considered the Quincecare duty or applied case law. She says that I have considered the case law on the basis that what happened here was an authorised push payment fraud but that was not the case.

  In my Provisional Decision I have made it clear that I have not reached any conclusion as to whether the payments were authorised or unauthorised, because I don't need to do so. I uphold the complaint on a different basis, namely that – whether the payments were authorised or not - the bank should have been on the lookout for the possibility of fraud and taken steps that could have prevented the losses to H.

  In this case, looking at what is fair and reasonable in all the circumstances of the case, I consider that Barclays failed to take appropriate steps to prevent the losses to H, and if it had acted as it should the fraud would have been prevented. I have explained this at length in the Provisional Decision. There is nothing in the responses from the parties that has persuaded me to reach a different conclusion.

- Miss Z is of the view that Barclays should fully reimburse all the losses incurred by H and not just 75%. She says that the disputed payments were unauthorised and made without H's apparent authority because the bank was "on inquiry" for believing that the transfers may have been an attempt to defraud H. So, it should not have allowed the payments without first verifying with H that the payments were authorised. She says that the bank failed to do so and therefore it was not entitled to debit the account of those payments. In other words, she considers that the bank should fully reimburse the losses for this reason.

  However, even if the transactions were to be considered as unauthorised, it is appropriate to take into account the Terms agreed between Barclays and H in relation to refunding the payments under such circumstances.

  The Terms state that if there is an unauthorised payment out of H's account, the bank will refund the amount unless H didn't take steps to keep the payment tools secure.

  Miss Z says that she did keep the payment tool secure. She has referred me to the Digital Channels Security User Guide which state that the administrators must keep their smart cards / Smart SIMs secure at all times and that means storing the card / SIM so only relevant user can access it. Miss Z says that this means the security is regarding the physical safety of the items. She says the payment tool was stored securely and was used by her following instruction from the bank (or so she thought).

  As I have said in the Provisional Decision, a key part of the requirement is certainly keeping the physical payment tools safe. But another part of the "payment tools" is "actions you [the customer] have to take", whether alone or in combination with the physical payment tools. Those actions include using passwords, security keys, cards, personal identifier(s), codes (such as Mobile PINsentry) fingerprints, and personal identification numbers (PINs).

  For example, if the customer discloses their PIN to a fraudster, that wouldn't be keeping it secure, even though a PIN is not a physical payment tool. Similarly, if the customer allows a third party to take control of payment tools by directing the customer's use of their PIN, card reader etc, in my view that also would be a failure to keep those tools secure. That is because, even though the physical payment tools may still be safely in

the customer's possession, the payment tools that consist of actions are placed under the control of the third party who dictates their use.

I have considered what Miss Z has said, but for the reasons I have explained in my Provisional Decision I remain of the view that in this instance the payment tools were not kept secure. This means that even if the payments were unauthorised, Barclays isn't obliged to refund the payments for that reason, under the Terms. But, as I explained in the Provisional Decision, that doesn't mean it is not fair and reasonable for me to uphold the complaint against Barclays for other reasons.

- Miss Z has also reiterated the sophisticated nature of the fraud and how the fraudster callously obtained Miss Z's trust as the bank employee, which she says was key to her subsequent actions. So, she says that it is not fair that H should bear 25% of the losses. She says that experiencing a fraud firsthand is quite different to looking at it subsequently as an 'outsider' and after the event.

  I appreciate what Miss Z says. However, in making a determination, I am required to base my conclusions on what I consider to be fair and reasonable in all the circumstances of the specific case.

  I have explained in detail in the Provisional Decision as to why I consider (as I still do) it is fair that H accepts some responsibility for the loss. Ultimately, Miss Z inputting the PIN to the log-in message allowed the fraudster access to the B.Net. After this, the payments started. All Miss Z could see was a blank screen and repeated instructions on her smartcard reader to enter the PIN. And then, to enter OK to the 'payment reference' shown on the reader. She saw these messages and input her PIN approximately 32 times. This went on for nearly three hours with her screen blank.

  This was an unusual occurrence. I think it is reasonable to expect that, as this went on and as she kept inputting the PIN without seeing how that repeated action was achieving what the caller promised her, she should have reflected on what was going on and taken steps to verify whether what the caller told her was indeed happening. Miss Z says that even if she somehow got visibility of the account, refunds don't usually appear instantly. However she would have seen that actually large payments were going out of the account following her inputting the PIN.

  I am not saying all this without sympathy for Miss Z and H for what happened. They fell victim to a callous fraud, and I am very sorry about that. I set this out only to give my reasons as to why I think it is fair that H bears some responsibility for the loss.

- As I said in the Provisional Decision, in cases like this, how the apportionment of the losses should be made is not an exact science. And I do recognise that requiring H to bear any proportion of the loss would impact it, especially given the sum involved. However, after weighing up everything, I consider it fair that Barclays reimburse 75% of the losses and the balance be borne by H.

Summary of my findings

(a) Even if the payments were unauthorised (about which I have not made a finding), Barclays isn't obliged to refund the payments for this reason under the Terms because H (or its representative) failed to take steps to keep the payment tools secure. However, there could be other reasons why it is fair that Barclays reimburses the loss to H.

(b) It is my view that the bank missed multiple opportunities to prevent the loss to H. So, I consider it fair and reasonable that it should compensate H for it.

However, I also consider that there was some contributory negligence on the part of H. Therefore, it is fair to allow for this in deciding the fair compensation. I consider that Barclays should reimburse 75% of the losses and the balance be borne by H.

(c) This matter caused considerable inconvenience to H. So, it is fair that Barclays compensates H for it.

(d) Ultimately, I must decide what is fair and reasonable in all the circumstances of the case. And, where I uphold a complaint, award such redress as I consider fair compensation, irrespective of whether a court would or would not award such compensation. Standing back and taking everything into account in this case, the compensation below is what I consider fair and reasonable.

Section E: Fair compensation

The fair compensation should be calculated as set out below:

1. Arrive at 75% of the loss under each of the two accounts. The loss will be the sum of disputed payments made from each account less the sum recovered to date under that account.

2. In relation to the business current account (account ending *4) calculate interest on the 75% of the loss on the account at 8% simple p.a. from the date of payments to the date of settlement.

   I consider this is fair because though the account earned little interest, the relevant question is the opportunity cost of the lost funds to H. In this case, I cannot be certain about the cost to H of being deprived of the money because it might have used the funds in a variety of ways. It is however clear to see that this was a large sum of money, and the loss has had a big impact on the company's finances. In the circumstances, without any compelling reason to depart from our usual approach, I consider it fair and reasonable that Barclays pays H simple interest at 8% p.a.

3. In relation to the interest-bearing premium account (account ending *1), calculate interest on the 75% of the loss on the account at the rate it would have earned had the money remained in the account, from the date of payments to the date of settlement.

   I consider this is fair because there was hardly any movement on the account prior to the fraud. So, it is reasonable to assume that the money lost on the account would otherwise have remained in the same account and earned the interest offered on the account.

4. £1,000 for the inconvenience this matter has caused.

5. Miss Z believes that Barclays should also pay H interest on the two £50,000 payments that went out of the account after the she advised the bank of the fraud and which have subsequently been recovered (so, they wouldn't form part of the loss amount above). She says that the payments shouldn't have happened in the first place, and then it took more than a month for the sum to be recovered.

   As I said in the Provisional Decision these two payments shouldn't have gone out in the first instance as the bank was already put on notice of the fraud. So I agree that it is fair that the bank pays H interest on these sums from the date of the payments to the date of recovery. Interest should be paid at 8% simple p.a.

6. So, I consider that the fair compensation is (1) + (2) + (3) + (4) + (5).

My final decision

Where I uphold a complaint, I can award fair compensation requiring a financial business to pay compensation of up to £375,000, plus any interest and/or costs that I consider appropriate. If I consider that fair compensation is more than £375,000, I may recommend that the business pays the balance.

Determination and award: I uphold the complaint. I consider that fair compensation should be calculated as set out above. My final decision is that Barclays Bank UK Plc should pay the amount produced by that calculation up to the maximum of £375,000 (including distress or inconvenience).

Interest awarded on the amount I've found payable as a money award is excluded from the award limit under DISP 3.7.5G. So, Barclays should also pay interest on that sum of £375,000 at 8% simple p.a. Given that most of the loss has arisen from the current account, I consider it fair that Barclays pay interest at this rate on the £375,000. Interest should be paid from 12 December 2022 to the date of settlement.

Recommendation: As the amount produced by the calculation of fair compensation as set out in the earlier section is more than £375,000, I recommend that Barclays Bank UK Plc pay H the balance together with balance interest.

This recommendation is not part of my determination or award. Barclays Bank UK Plc doesn't have to do what I recommend. It's unlikely that H can accept my decision and go to court to ask for the balance. H may want to get independent legal advice before deciding whether to accept this decision.

Under the rules of the Financial Ombudsman Service, I'm required to ask H to accept or reject my decision before 7 November 2024.

Raj Varadarajan
Ombudsman