

The complaint

M, a limited company, is seeking to recover £12,744.35 from Barclays Bank UK PLC (“Barclays”), which was stolen from its business banking account as a result of a third-party scam.

The owner of M, Mr G, is bringing the complaint on its behalf so I will refer to him throughout.

Barclays says it is not liable for the loss because Mr G unwittingly authorised the payment himself — and it could not reasonably have intervened or done more to try to recoup the money from the receiving bank once it had become aware of the scam.

What happened

The details of the complaint are well known to both parties so I won’t go into too much detail here. However, in summary, Mr G’s business, M, has been the victim of a scam. Mr G was tricked into sending £12,744.35 to whom he thought was a business he had a long-standing agency relationship with and who he had made regular payments to before – which I will refer to as X.

In May 2019, Mr G received numerous emails which appeared to come from X. The contents of these emails discussed an audit that X was going through, outstanding amounts owed by M and which account these outstanding amounts should be paid to. Mr G was asked to make a payment to an account that differed from the usual account he transferred to at X. The email including the updated account details appeared in a chain of conversation that Mr G had been responding to and appeared to come from a person he had previous contact with at X.

So, on 21 May 2019, Mr G transferred the money as per the instructions he was sent in the email. He did so via online banking. He has told us he set up a new payee to make the payment.

However, some days later, Mr G was contacted by the genuine X who enquired when he was intending to make payment. It then came to light that X had not sent the emails containing the updated account details. And the payment had not been paid into their account. Mr G had fallen victim to a sophisticated scam - the email Mr G received was from a fraudster who had managed to send fake emails to Mr G – which looked just like genuine ones sent by X and which appeared to come from the same email address.

Mr G contacted Barclays to make them aware of the scam and Barclays raised an indemnity with the receiving bank the same day. However, the receiving bank confirmed that no funds remained in their account. Mr G also instructed his solicitors, who wrote to Barclays setting out why they believed M should be provided with a refund. Mr G and his representatives felt that Barclays could’ve, and should’ve, done more to protect M from this type of fraud and that M should now be offered a refund under the recently introduced

Contingent Reimbursement Model (the CRM Code) which Barclays was a signatory to. Mr G also contacted Action Fraud and the police.

During the course of the police investigation, Mr G was told that £6,000 of his money had remained with the receiving bank. Mr G was told to contact Barclays again and request a further indemnity be raised so this money could be returned to M's account. Ultimately, both Mr G and the police contacted Barclays about raising a further indemnity to get this money returned but Barclays declined to contact the receiving bank again – reiterating that it had previously been told that the funds had already been removed from the account.

As a satisfactory resolution could not be reached, Mr G brought his complaint to our service. Mr G added that he felt Barclays' failure to respond to letters from his solicitor was deliberate. Mr G told our investigator that his solicitors had sent detailed letters on numerous occasions and Barclays had failed to engage with these or even respond – choosing to contact him directly instead despite him having requested contact via his solicitors only.

Mr G went on to say that he had done his own research and it had become apparent to him that a system known as Confirmation of Payee ("CoP") was due to be introduced across the banking industry but had been somewhat delayed. This system would tell customers who were making online transfers whether the name they had been given by the payee matched the name of the recipient account holder. Mr G said that without this, there was no way for a bank to cross-check whether a customer's funds were being transferred to an account in the correct name. Mr G said he had assumed that when he entered the account name to make the payment now in question, this crosscheck was already taking place. Mr G has said that had he known this wasn't the case - specifically had he been informed of this by Barclays - he would've taken more steps to verify the payee account and the scam would've come to light and ultimately been prevented.

One of our investigators reviewed the complaint but didn't uphold it. She didn't think M was entitled to a refund under the CRM Code as it was not in place at the time Mr G made the payment and it was not retrospective. And she made the same point in relation to the arguments Mr G had put forward in relation to CoP – it wasn't a system that was in place at the time so Barclays wouldn't have been able to check the account name that the funds were being transferred to. She didn't think it would be fair and reasonable to say Barclays should've done something that it wasn't in fact able to do at the time. She also didn't think the transaction Mr G made was unusual and out of character when compared to M's usual account activity and so she didn't think there would have been a reason for Barclays to have questioned Mr G about the payment before they allowed it to leave M's account either.

The investigator went on to say that she had seen the messages shared between Barclays and the recipient bank and could see that the recipient bank had confirmed that no funds had remained in the account by the time they had been contacted by Barclays. She did, however, acknowledge that the recipient bank now appeared to have told the police something different. She told Mr G she intended to discuss this further with the receiving bank.

Mr G didn't agree with the investigator's findings. He put forward the following arguments:

- He had received a text from Barclays asking him if he made a payment to X shortly after the payment was made. Mr G said this text message used the payee name he had entered into the online banking system. Mr G says this reinforced that the payee account name was legitimate. Mr G pointed out that it would've been relatively easy

for Barclays to warn customers in this message that this was the name entered by the user and was not an indication of the actual account name.

- He should now receive interest on the £6,000 payment that was being held with the third-party bank as Barclays had failed to action his request to raise a further indemnity and M had continued to be without funds unnecessarily.
- Whilst the payment now in question wasn't particularly unusual for the account, all the other payments made from the account were to existing payees.
- He understood that Barclays didn't have a CoP facility in place at the time but as they were aware of a flaw in the UK banking system, they should have warned their customers of this failing. Mr G said it should be for this service to raise standards across the banking sector.
- Barclays had failed throughout the course of the investigation to engage with his solicitors and Mr G now wanted his legal costs refunded.

Our investigator reviewed the complaint again and, in the main, her opinion remained the same. However, she had spoken to Barclays again and it had agreed to raise a further indemnity with the receiving bank - who had confirmed it was holding £6,000 on behalf of M.

Our investigator agreed with Mr G that this should have been done sooner and that Barclays should pay interest on this amount at a rate of 8% simple per annum. Barclays agreed and completed the necessary calculation. However, there was an error in the original interest calculation which was pointed out by Mr G. Barclays acknowledge the error, rectified it and paid a further £100 in compensation – which Mr G accepted on behalf of M.

However, as an overall agreement has still not been reached, the complaint has been passed to me for a final decision.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In deciding what's fair and reasonable, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

I'm really very sorry to hear about what's happened to M. I also have significant sympathy for the situation Mr G has found himself in. But having thought very carefully about what he's told us happened at the time and Barclay's actions, I'm not persuaded it would be fair and reasonable for me to hold Barclays liable for M's loss.

So, having considered everything, I won't be upholding M's complaint. I do appreciate how disappointing this will be for Mr G, but I don't think I can fairly say that Barclays should reimburse him with the money his business has unfortunately lost to the scammers. I'll explain why.

Mr G has requested that M's case be considered, and M be compensated, under the CRM Code. This is a voluntary scheme Barclays has signed up to, designed to reimburse customers that have fallen victim to a scam. However, the code didn't come into force until 28 May 2019 – a week or so after the payment in question here was made. As the code is not retrospective, it isn't applicable to M's circumstances and I'm not persuaded it would be fair and reasonable to hold Barclays liable under a code that wasn't in place at the time. And so I've then gone on to think about what was in place at the time.

In broad terms, the starting position in law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the terms and conditions of the customer's account. However, 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, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.
- For branch transactions, those steps may include following the Banking Protocol where appropriate.

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.

So, in this case, I need to decide whether Barclays acted fairly and reasonably in its dealings with M when Mr G transferred £12,744.35 to a fraudster and when he reported the fraud, or whether it should have done more than it did.

It is not in dispute that Mr G authorised the payment himself. Because of this, Barclays had an obligation to follow his instructions. But there are some situations in which it should reasonably have had a closer look at the circumstances surrounding the transfers - as I've explained above. I consider that as a matter of good practice Barclays should've been on the lookout for unusual and out of character transactions.

So, I've then thought about whether the transfer Mr G made could be considered out of character and unusual when compared with M's usual account activity. I've reviewed M's account statements for the months leading up to the scam, and I'm not persuaded it was. M had made similar payments in the months prior to the scam. For example, M had completed the following transactions:

- 31 January 2019 – a bill payment of £31,008.12
- 22 February 2019 – a bill payment of £16,800
- 29 March 2019 – a bill payment of £38,306.66
- 3 May 2019 – a bill payment of £27,601.88

And so, I'm not persuaded it would be reasonable for me to say that a payment of £12,744.35 was unusual for M – it had carried out very similar (and higher) transactions in the months before.

I've also thought about the fact the payment was sent to a new payee. However, I don't find that a payment to a new payee is in itself suspicious enough to mean that Barclays should've considered that M was at risk of financial harm and contacted Mr G before it made the payment at his request.

It is important for me to stress that banks have to strike a balance between processing payments as per their customer's instructions and monitoring accounts for unusual and potentially harmful activity. And I don't think it would be fair to say that Barclays should've identified the payment Mr G made as suspicious enough to warrant further checks – especially given that M had a relatively high outstanding balance and the account often made large payments.

I've also thought about whether Barclays could've done more to help M once it was notified of the scam and following the police investigation – I think it could. Barclays contacted the receiving bank upon notification of the scam. But, unfortunately at this point, it was told M's funds had already been removed by the scammer. And so, I understand why Barclays told Mr G this at the time. However, it later came to light that a £6,000 payment had been refunded back into the account - which is why the investigating police officer was told something different to Barclays. Despite being notified of this by both Mr G and the police, Barclays declined to engage with the updated information provided by the receiving bank and raise a further indemnity. And I think it should have done. Had it done so, I'm persuaded that this amount would've been returned to M much sooner than it ultimately was. However, having said the above, I can see that Barclays has now paid M compensation for the amount of time it was without the funds. And as Barclays has already paid what I would look to recommend in these circumstances, I won't be recommending it pay anything further.

I've also thought carefully about what Mr G has said about Barclays failing to warn him, and other customers, that a 'Confirmation of Payee' system was not in place at the time and that it could not verify whether the name of the account holder entered into its payment system matched the payee account name. And whilst I acknowledge that this system was due to come into place, there was no obligation for Barclays to inform its customers that it wasn't already. And I don't think it would be fair for me to hold Barclays to a standard that wasn't in place at the time. It is the Financial Conduct Authority ("FCA"), the regulator of financial services in the UK, who are responsible for regulating the conduct of businesses and setting rules for businesses to follow, not the Financial Ombudsman Service.

The text message received by Mr G shortly after the payment in question was made was to highlight to Mr G that a new payee had been set up on the account and a payment made to it - should this activity have been unauthorised, the text message would've made Mr G aware of the unauthorised activity on his account, so the payment could be stopped and the account blocked. The purpose of this text message was not to confirm or reinforce that the correct payee name was being used although I appreciate this is what Mr G felt it did.

Finally, I've thought about whether Barclays should be liable to pay M's solicitors fees. But I don't think it should. It was Mr G's choice to instruct legal representation and he could've gone through Barclays' complaint process and brought his complaint to this service without doing so. I appreciate that Mr G feels Barclays did not engage with the letters sent by his solicitors. However, Barclays has said some letters were sent to addresses not used for incoming correspondence and it has apologised for not responding to those received. Ultimately, I'm not persuaded that this has had a material impact on the outcome of this complaint. Had Mr G's letters been received and responded to, Barclays position would've likely remained the same. And Mr G could've brought his complaint to this service had he received a response or not – once the required amount of time had

passed. So I won't be recommending that Barclays pay for services Mr G chose to instruct and ultimately pay for.

I want to stress that my role in deciding this case is not to assign blame. It's clear that Mr G has unfortunately been a victim here. I am very sorry to hear about the situation he has found himself in. But at the same time, I don't think his and M's loss was caused by any specific failing on behalf of Barclays. The fault here lies with the cruel and callous acts of the fraudsters themselves.

My final decision

For the reasons I've explained, I do not uphold this complaint against Barclays Bank UK PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask M to accept or reject my decision before 28 January 2022.

Emly Hanley
Ombudsman