DRN-3457715

The complaint

K, a mutual society represented by Mr R, complains that Barclays Bank UK PLC did not refund all of the money K lost when it fell victim to an email interception scam.

What happened

The facts of this case are well known to both parties so I will summarise the key details here.

K's email account was compromised, leading to an invoice from a contractor being intercepted and the bank details for the payment being changed. This meant the payment of just over £47,000 made from K's account with Barclays went to a fraudster and not to the contractor.

Mr R has explained that K operates an internal payment system where two colleagues are involved with the payment of invoices and no colleague was concerned about this particular invoice at the time. Mr R said the contractor was new and K had received emails from both the contractor and the quantity surveyor advising of a change of bank details. Mr R explains that the email came from the contractor's genuine email address.

When the scam was uncovered, Mr R contacted Barclays. He pointed out that the fraudsters account was also with Barclays and he wanted to know why the bank had allowed a fraudulent account to be set up.

Barclays said the fraudster had used the funds before K reported the scam. But the bank had not promptly logged a scam claim for K when it should have done. Barclays refunded 50% of the money K had lost due to this error.

But Barclays said it was not responsible for refunding the rest of the loss. In its final response letter, it said K did not carry out effective due diligence to ensure it was fully aware of whom it was paying. It said the scam invoice had account details crossed out in pen and K should have phoned the contractor to confirm if it had requested payment be made to a new account. The bank said it had given an effective warning about invoice scams to K at the time the payment was made and K ignored this information.

K was unhappy with Barclays' response and referred a complaint to this service. Mr R explained that the account details on the scam invoice were crossed out by K after the scam came to light and not by the fraudster. He pointed out that he'd been expecting the contractor to send an invoice with new bank details because of the previous correspondence that had been received from a known email address.

Our Investigator looked into the complaint and recommended that it should be upheld. He explained that under the terms of the Lending Standards Board's Contingent Reimbursement Model (The CRM Code), Barclays should reimburse K unless one of the CRM Code's exceptions applied. He didn't think any of the exceptions were applicable here. He didn't agree the warning Barclays had shown was impactful in K's circumstances and he thought it was reasonable for K to believe it was making a legitimate payment to its contractor.

Barclays disagreed and asked for an Ombudsman to review the complaint, so the matter has been referred to me. Barclays was concerned about the security measures K had in place. It pointed out that K had made a genuine payment to the contractor a month before and said it should have checked the change in account details before making this payment. It felt K missed clear opportunities to challenge and question the payment before it was made. It felt the warning the bank gave to K was effective and the staff member that saw it should have discussed it with Mr R before completing the payment.

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.

Barclays was both the sending and the receiving bank for the payment at the heart of this complaint. In this decision, I have only considered Barclays' actions as the bank that sent the funds. Having done so, I think that Barclays should have refunded the full amount of the payment K made. The payment K made was covered by the CRM Code and I am not persuaded any of the permitted exceptions to full reimbursement under the CRM Code apply in the circumstances of this case. I'll explain why.

The starting point in law is that K is presumed liable for any transaction it authorises. It's not unusual for K to make large payments to pay invoices and so at the time this payment was made, K authorised it. This is the case even though it was later discovered that K had been tricked into doing so. But Barclays has signed up to the CRM Code. The CRM Code says that firms should refund customers that fall victim to an authorised push payment scam like this one except in a small number of circumstances.

Barclays' arguments have focused on the warning that was presented to K at the time the payment was made. It says that K failed to meet its level of care under the CRM Code because it ignored an "*Effective Warning"* that applied to the payment being made.

The CRM Code says that where firms identify APP scam risks in a payment journey, they should provide Effective Warnings to their customers. Barclays says that K's employee specified that K was making a payment to pay an invoice and was presented with the following information:

"Could this be a scam?

Was this invoice unexpected? Does it have new account details? Fraudsters have been known to intercept genuine correspondence, including text messages, and change the account details to their own.

That's why we recommend checking the details of where you're sending the money to in person. If you were contacted by phone to pay this invoice, use a different phone to call the company so the call can't be diverted."

The CRM code says that for a warning to be an Effective Warning, it must be (at a minimum), understandable, clear, impactful, timely and specific.

Whilst the information Barclays presented is designed to be relevant to the scam K fell victim to, I am not persuaded that it is specific and impactful enough to meet the requirements of an Effective Warning and I am not persuaded that K ignored an Effective Warning by failing to take appropriate action in response to it.

The warning starts by advising caution about invoices that are *"unexpected."* This is not how

scams of this nature tend to unfold. Fraudsters typically replace a genuine and expected invoice with a fraudulent one, which is what happened here. K was expecting to receive an invoice for payment from its contractor and it was also expecting to pay the contractor using new account details because of the emails it had received previously from both the contractor and the quantity surveyor. I can see why a customer reading this warning who had not received an invoice out of the blue might reach the conclusion that the information was not relevant to them. And in the circumstances of this case, I can see why the change in account information did not cause alarm with K's staff and why K proceeded with the payment without any further internal discussions.

Barclays has suggested that its inclusion of the phrase *"genuine correspondence"* in the warning applies to emails from genuine email addresses. But the bank has a far superior knowledge of what scams like this look and feel like. At the time of the scam, K did not, and I don't think the information Barclays provided did enough to make K aware of the risks.

Confirming account details in person or over the phone with the sender is almost always sufficient to prevent this type of scam. So, it's crucial that the importance and relevance of doing this is explained (as well as the consequences of not doing it). The warning does mention contacting someone 'in person' (which, if taken literally, could be an impractical step in many circumstances) but the warning fails to stress the importance of speaking to the sender directly or what the consequences of not doing so could be. By not doing this, the warning lacked impact and was less likely to be effective for customers in K's position.

The warning also fails to really bring alive what a scam of this nature looks like - how a fraudster can gain access to and monitor email accounts so as to impersonate someone and send emails from their email address (or something which looks very similar). By failing to do this, it makes it much easier for a customer, like K, not to recognise their own circumstances in the warning. That may have been what happened here. K has explained that it believed the correspondence was genuine because the fraudulent email and invoice looked identical to genuine correspondence.

Overall, I don't think K ignored an effective warning or that it was unreasonable for K to proceed with making the payment having seen this information.

I've thought about whether any of the other specific exceptions to reimbursement under the CRM Code could apply here. Over the course of the complaint, Barclays has made comments suggesting K made the payment without having a reasonable basis for believing that the payee was the person K was expecting to pay, the payment was for genuine services and/or the person or business with whom K transacted was legitimate. But I'm not persuaded that Barclays' concerns are enough to establish that K failed to meet its level of care.

From what I have seen, it would have been very difficult for K, or anyone else, to tell that it had received a fraudulent invoice. The only change to the format of the invoice was the substitution of the account details. There was also no reason for K to think it wasn't communicating with the genuine contractor or that the payment request hadn't come from them. K was anticipating receiving new account details so receiving the invoice did not arouse any concern and nor do I think it ought to have done. The mere fact that K could have checked the account details over the phone with the contractor before making the payment does not equate to a finding that K lack a reasonable basis for belief.

From what I have seen, I am satisfied that there was no particular reason for K to find the payment request unusual or to doubt its authenticity. I don't think it was unreasonable for K to have made the payment in the circumstances that it did.

Overall

The CRM Code explains that where a customer has met their requisite level of care (which as I've explained, I'm satisfied was the case here) they should be refunded all of the money that was lost. So I think it's fair that Barclays now refunds the remainder of the money K lost, along with interest as I've outlined below.

My final decision

For the reasons I've explained, I uphold this complaint about Barclays Bank UK Plc.

To put things right, Barclays Bank UK Plc should now:

- Pay K a refund of the money that was lost to the scam, less any funds it has been able to recover and any redress that it has already paid

- Pay 8% simple interest from the date Barclays declined K's claim under the CRM Code until the date of settlement

If Barclays considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell K how much it's taken off. It should also give K a tax deduction certificate if it asks for one, so K can reclaim the tax from HM Revenue & Customs if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask K to accept or reject my decision before 30 August 2022.

Claire Marsh
Ombudsman