DRN-3372966

The complaint

Mr M is unhappy that Barclays Bank UK PLC won't refund all the money he's lost to a scam.

What's happened?

Mr M had been communicating with his appointed conveyancing solicitor ('the solicitor') via email since November 2020.

On 9 March 2021, contracts were exchanged regarding Mr M's property purchase and he transferred a 10% deposit to the solicitor via online banking. On the same day, the solicitor confirmed in an email that the house purchase would complete by 31 March 2021, and the outstanding balance would need to be paid prior to that date.

On 11 March 2021, Mr M says the solicitor called him to let him know that another of their clients had received a scam email asking them to make a money transfer. Mr M says the solicitor's warning was general and without context.

On 15 March 2021, Mr M received an email requesting payment of the outstanding balance. The email appeared to come from the solicitor and followed-on in the same email chain between the solicitor and Mr M from earlier in the month. Mr M says the payment request was expected, everything looked the same as it had always done, and nothing stood out to him as suspicious. Payment of the outstanding balance was the last stage in the process of purchasing his house, and everything had gone smoothly so far.

Attached to the email was a letter which cited the account details Mr M should send payment to. Mr M says the letter looked official – it contained the correct company logo and address. He noted that the letter asked him to pay the outstanding balance to different account details than he had used before when he'd paid the deposit, but he didn't think anything of this – he assumed it was because of the security breach the solicitor had alluded to on 11 March 2021.

Mr M made two payments of £50,000 to the account details he'd been given. The first payment went through successfully, but the second payment was stopped. Barclays contacted him and asked him to check the payment details with the solicitor before the payment was processed. When he called the solicitor, they said they hadn't requested payment of the outstanding balance, and it became apparent that he'd been the victim of an email interception scam.

Barclays accepted partial responsibility in this case and reimbursed half of Mr M's loss - £25,000. It said that both of the £50,000 payments Mr M instructed on 15 March 2021 were flagged for further checks by its fraud detection system, but its fraud team only called Mr M to discuss the second payment. So, it could have done more to protect Mr M from financial harm by contacting him to discuss the first payment too. But Mr M:

- ignored the relevant scam warning it gave during the payment journey.
- ignored the verbal warning that the solicitor gave him on 11 March 2021.
- ought to have known about the possibility of email interception due to the nature of

his employment.
- should've done more checks before making payment – for example, checking and confirming the account details with the solicitor and/or making sure the email he'd received was genuine.

Barclays contacted the receiving bank on the day the scam occurred, but no funds remained in the beneficiary account to recover.

Mr M would like to be fully reimbursed for his loss, and he has asked this Service to consider his complaint.

What did our investigator say?

Our investigator thought that Barclays should've fully reimbursed Mr M under the provisions of the Lending Standards Board's Contingent Reimbursement Model ('CRM Code'). Barclays didn't agree, so the complaint has been passed to me to decide.

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 is a signatory of the CRM Code, which requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr M has fallen victim to, in all but a limited number of circumstances. Barclays has argued that two of the exceptions apply in this case. It says that Mr M ignored an effective warning it gave during the payment journey and he made the payment without a reasonable basis for belief that the payee was the person he was expecting to pay, the payment was for genuine goods or services and/or the person or business he was transacting with was legitimate.

The CRM Code says:

SF1(2)(e) As a minimum, Effective Warnings should meet the following criteria

(i) Understandable – in plain language, intelligible and meaningful to the Customer
(ii) Clear – in line with fair, clear and not misleading standard as set out in Principle 7 of the FCA's [Financial Conduct Authority] *Principles for Businesses*
(iii) Impactful – to positively affect Customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced. This should include steps to ensure that the Customer can reasonably understand the consequences of continuing with an irrevocable payment;
(iv) Timely – given at points in the Payment Journey most likely to have an impact on the Customer's decision-making;
(v) Specific – tailored to the customer type and the APP scam risk identified by analytics during the Payment Journey, and/or during contact with the Customer.

Barclays says it gave Mr M the following warning during the payment journey:

"House or large purchase"
"Have you double checked the account details with the person/company you're paying? Fraudsters have been known to intercept emails from solicitors 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."

I've considered the warning and, overall, I'm not satisfied it can reasonably be said that the requirements of the effective warning exception were met. I appreciate that the warning was relevant to the type of scam Mr M fell victim to. But I don't think it was impactful enough to affect a customer's decision making in a manner whereby the likelihood of this scam succeeding was reduced.

It's clear to me that Barclays' warning attempts to prevent email interception scams, and I think it sets-out the risk quite well. It says that fraudsters can intercept emails and change the payment account details and it recommends that customers double-check payment account details in person. But I don't think the warning goes far enough to make the risk really obvious to customers. It doesn't bring to life what this type of scam looks like, nor does it talk about the prevalence of this type of scam or explain how sophisticated the scams can be. For example – it doesn't explain that fraudster's emails appear to come from the same address as the account they've hacked, that they can communicate with their victim on a genuine chain of emails, that fraudulent emails are usually received when a payment request is expected or that fraudster's emails can seem genuine and look the same or very similar to the person's they're impersonating.

Overall, I'm not satisfied that a reasonable person would fully understand the scam risk from the warning Barclays gave.

The circumstances of this scam made the warning even less effective. Mr M had been communicating with the solicitor via email for many months. They were at the last stage in the process of purchasing a house and everything had gone smoothly so far – including the deposit payment which had been made via bank transfer after receiving payment instructions via email. Mr M received a payment request he was expecting to receive, in an email which looked the same as the solicitor's emails and followed-on in a chain of genuine emails. To him, everything looked the same as it had always done, and nothing stood out as suspicious. From what I've seen, I don't think Mr M appreciated the risk that the email may have come from a fraudster that was tricking him into making a payment to them. This is supported by Mr M's testimony that he saw Barclays' warning and double-checked the account number and sort code he'd been given against his payment instruction in response to it. It appears he thought it was enough to check he'd got the payment details right by looking at the email he'd received. If Barclays had really brought to life what a scam of this nature looks like then I think that would've been important information in the context of this scam that would've affected Mr M's decision making and led him to take additional steps to protect his assets – such as telephoning the solicitor to verify the account details, particularly as he'd noticed they'd changed.

In addition, I note that the first payment triggered Barclays' fraud detection system, but it didn't contact Mr M to ask him further questions about the payment or advise him of the scam risk. If it had done so, I think it's likely that it would have asked Mr M to contact the solicitor to check the payment details, as it did with the second payment. And Mr M would have taken the required action, as he did with the second payment. So, the scam would've unravelled without the first payment being made and Mr M's loss could've been prevented.

From what I've seen, I'm satisfied that Mr M had a reasonable basis for belief in this case. He says he had a lot going on at the time – home schooling his children during the pandemic and preparing to move house – and nothing about the fraudulent email stood out to him as suspicious. From what I've seen, I can understand why. Barclays has said that Mr M just assumed the email was genuine because it looked genuine, and he didn't carry out any extra checks. But I don't think this is unreasonable in the circumstances, particularly as Barclays hadn't adequately explained the fraud risk to him.

I accept that the solicitor warned him about scam emails asking for money transfers. But the warning appears to have been general in nature. From what Mr M's said, it didn't fully explain the fraud risk or bring to life what a scam of this nature looks like – for example, the solicitor didn't explain that scam emails would look like they came from them. So, I don't think it's unreasonable that Mr M's suspicions weren't roused when he received the fraudster's email. This is particularly so given that the fraudulent email looks the same or very similar to the solicitor's genuine emails, appears to come from the solicitor's email address, was sent at a time when a payment request from the solicitor was expected and follows-on in a chain of genuine emails between the solicitor and Mr M.

I also appreciate that Mr M noticed he was being asked to pay a different account to the one he'd paid previously. But I think his assumption about the reason for this was reasonable in the circumstances.

Barclays has said that Mr M ought to have known about the risk of email interception due to the nature of his employment. I'm not persuaded by this argument. I think it is based on a sweeping assumption. But in any event, Mr M says Barclays isn't correct about his employment role – he actually works in financial services. I don't think there's any indication that Mr M ought to have had any special knowledge about the possibility of email interception scams.

Overall, the fraud was sophisticated, and I can understand why it went undetected by Mr M.

My final decision

For the reasons I've explained, my final decision is that I uphold this complaint and instruct Barclays Bank UK PLC to:

- reimburse the remainder of Mr M's loss – £25,000 – within 28 days of receiving notification of his acceptance of my final decision; plus
- pay 8% simple interest per year on that sum from the date of the payment to the date of settlement.

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

Kyley Hanson
Ombudsman