DRN-2359186

The complaint

Mr and Mrs R seek to recover about £46,000 from Al Rayan Bank PLC, which was stolen from their bank account in 2019 as a result of an invoice interception scam.

What happened

In October 2019, Mr R was looking to buy a property. Following email correspondence with his solicitors, M Limited, he made the following payments in a branch of the bank:

Date	Location	Transaction description	Amount
08/10/2019	Al Rayan Bank Branch	Genuine faster payment sent to "*M Limited"* made over the counter in branch.	£16,452.00
10/10/2019	Al Rayan Bank Branch	Faster payment again processed over the counter in branch, made to a slightly different account in the name of "*M Client".*	£148,066.30

The payment made on 8 October 2019 was a legitimate payment and reached M Limited's account with no problem.

However, in between the two payments, Mr R received an email supposedly from M Limited. This email instructed him to change the account details and the company name when making the second payment. Unbeknown to him, this email was sent to him by fraudsters, pretending to be from M Limited. So, on 10 October 2019, he unwittingly sent the £148,066.30 to the fraudsters' account instead of M Limited. Both payments were completed in branch with the help of the same cashier. Mr R says that he was only asked what the payment was for – which he responded to by explaining it was for a property purchase. On both occasions, he was given a payment slip to sign as a receipt.

But after sending the second payment, Mr R received a call from Al Rayan Bank to inform him that the wrong payment type had been attempted in branch. The cashier had tried to put through a *Faster Payment;* when in fact a *CHAPS* payment was required as the amount was over £100,000. Mr R was told that he needed to pay a £15 fee to send the money in this way and has said he was not asked any further questions about the payment, nor were the details of the intended beneficiary discussed. The CHAPS payment was successfully sent shortly afterwards.

A little after this, Mr R contacted M Limited to find out about the payment and the progress of the property purchase. He explained that he'd sent the payment that same day – but M Limited advised that the funds hadn't been received. It was at this point that Mr R realised that he'd been the victim of a scam and someone had intercepted his emails. So, he immediately contacted Al Rayan Bank to try and stop the payment to get his money back.

Unfortunately, the payment had already left Mr R's account and had been sent to the scammers. Al Rayan Bank contacted the receiving bank and a total of £102,045.07 of the payment was successfully recovered – but the remaining £46,021.23 was lost.

Al Rayan Bank declined to refund the *c.*£46,000 back to Mr R. It said that the responsibility falls on him for transferring the money to the account details he gave to the cashier in branch. Because Al Rayan Bank staff had sent the payment to these exact details as directed, it cannot be held liable for the payment as it was authorised. It also said that it had done all that was reasonably possible to help recover the payment from the beneficiary bank.

Unhappy with this, Mr R raised a complaint. He cited that Al Rayan Bank ought to have done more to help identify this was a scam, especially as invoice interception is a well-known technique used by fraudsters. He managed to go ahead with the property purchase, but only by borrowing money from friends and family. Again, Al Rayan Bank maintained that it had not acted unfairly.

Mr R disagreed and therefore brought the complaint to our service. One of our investigators looked into it and, ultimately, thought that Al Rayan Bank missed opportunities to stop the payment before it was made, especially as it was an out of character transaction for the account. In his opinion, Al Rayan Bank hadn't gone far enough to probe into the legitimacy of the payment, namely because it merely asked what it was for. And if it had probed further, he was persuaded that the payment would've been prevented. Therefore, he upheld the complaint and recommended that Al Rayan Bank refund Mr R what was left outstanding from the £148,066.30, plus interest. Mr R agreed with this recommendation.

Al Rayan Bank does not agree. It submits that:

- Mr R should be held liable for the payment because he authorised it, and the branch staff member simply followed his instruction to process the payment to the account details provided.

- The bank disputes that the payment should've stood out as uncharacteristic, because the payment made on 8 October 2019 held similarities. As such, the second was not suspicious.

- Finally, Al Rayan Bank accepts that the beneficiary name/title differed between the two payments. But nevertheless, it's common for solicitor firms to hold multiple accounts and to operate under slightly different names. And its staff searched a well-established register for legal/solicitor practices to validate the legitimacy of M Limited.

Because Al Rayan Bank does not agree, the complaint has been escalated 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.

Under the Payment Services Regulations 2017 (PSRs), and in accordance with banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even if they were duped into giving that authorisation or it was obtained by third-party fraud.

It's common ground that this was an 'authorised payment', even though Mr R was the victim of a sophisticated scam. He used his security credentials to request the payment. So, although he did not intend for the money to go to the scammers, under the PSRs, and the terms and conditions of his account, Mr R is presumed liable for the loss in the first instance.

However, taking into account the law, regulator's rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Al Rayan Bank 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 make 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 like the one in dispute here, those steps may include following the Banking Protocol where appropriate.

The Banking Protocol is a multi-agency initiative between the Police, financial sector organisations (including banks, building societies and the post office) and Trading Standards *'aimed at identifying customers who are in the process of being defrauded and implementing safeguarding procedures to prevent their repeat victimisation and further loss of funds'*. It has been fully in force since March 2018.

In broad terms, according to UK Finance's toolkit for payment service providers, financial businesses commit to:

- Look out for any unusual or out of character withdrawals and to implement the Banking Protocol procedure when such transactions are identified.

- Discreetly question the customer about the withdrawal or transaction and their reasons for making it, keeping in mind that the customer may have been told they are helping to catch a corrupt bank employee and may have been given a cover story to tell if asked about the transaction.

- Consider the responses against what they expect as normal activity on the individual's account. If they are concerned or suspicious that the customer may be the victim of fraud, they should notify a senior member of staff, who should take the customer to a quiet area and ask further questions to establish more details.

- If the senior colleague believes the customer is the victim of fraud, either as a result of the answers provided or through their general behaviour, they should call the Police immediately who will attend the branch to speak to the customer.

The Banking Protocol procedures are not limited to elderly or vulnerable customers, or certain fraud types, and bank staff are encouraged to contact the police even if they are not sure. It reflects good industry practice at the material time.

So, in accordance with the law, regulations and good industry practice, a bank has a duty to protect its customers against the risk of fraud and scams so far as is reasonably possible. Amongst other things, this might involve a bank looking to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam.

Al Rayan Bank submits that the legitimate payment to M Limited two days' prior is comparable to the later payment that's in dispute. For that reason, it doesn't agree that the payment made on 10 October 2019 should've been flagged as suspicious. But I'm not satisfied that the legitimacy of the first transaction means that the payment on 10 October 2019 should have just gone through without appropriate checks.

I accept that both transactions were thought to be to solicitors for a property purchase. But the payment on 10 October 2019 was for £148,066.30 – *more than eight times* the amount of the first one and a significant sum in its own right. Whilst not inherently unusual or uncharacteristic in the context of a known property transaction, it still merited some discreet checks before processing because of its size and because scams of this nature are well-known to the banking industry (hence the need for the Protocol).

The key point here is that both payments were processed in the same branch by the same employee. I accept that he would have not regarded a large payment shortly after a smaller (but significant) payment as odd in the context of a property purchase, especially as the earlier one hadn't been queried by the customer authorising the current payment in person. However, the second payment contained features that were unusual or uncharacteristic and, in my view, could and should have been picked up by the bank given its knowledge of common fraud and scams. A new payee had to be set up in order for the payment to be sent supposedly to the same firm of solicitors. This was a completely new account and this new payee had a different *name*. I think that should have rung alarm bells in branch, as invoice intercept scams are so well known.

I accept that the two account titles – i.e. "*M Client"* instead of *"M Limited"* – were only slightly different. But there were different sort codes and account numbers. They were clearly different accounts – and that should have raised suspicions if Mr R was simply completing a property purchase by remitting funds via the same solicitors. I accept that such information would not itself reveal fraud, as a firm may indeed hold and use multiple accounts. But it would justify the asking of questions to Mr R, which would probably have led to the disclosure of the 11th-hour email requesting the change of banking details – and this would probably have alerted the bank given the prevalence of this type of scam. It could then have warned Mr R or, indeed, even stopped the transaction until it was satisfied everything was okay.

The bank says its staff checked the firm of solicitors on the Law Society website. But that is patently a futile exercise in the context of this sort of scam. There is no dispute that M Limited was a legitimate firm acting for Mr R. Checking their credentials with the Law Society doesn't help when a scammer spoofs their emails or sets up a false account with a similar-sounding name.

An internet search was poor protection in such circumstances. What the branch staff should have done is ask Mr R about the last-minute change in details; explain that this might indicate a common scam; and advise him to double-check with his solicitors via another channel, e.g. phone. If they'd done this, the scam would have been exposed before it was too late.

If Mr R had found the questions intrusive or refused to cooperate or insisted on the transaction proceeding regardless, then he would only have had himself to blame and we would not be asking the bank to cover the loss. But the point is, he was denied this opportunity because the bank asked insufficient probing questions about a transaction that ought reasonably to have been identified as inherently suspicious due to the last-minute change of details for the 'same' payee.

According to Al Rayan Bank's records, they merely asked Mr R where the money was going. In my judgment, they could and should have done more; particularly, given the requirements of the Banking Protocol which encourages staff to ask probing questions and to get into the detail in order to test the purpose of the payment. Mr R hadn't been given a cover story by scammers; and he seems to be honest and straightforward – so would have answered the bank's questions truthfully and, more likely than not, spoken of the email requesting the change. He might even have shown it to the bank, which would then have given both of them an opportunity to look more closely at it (and thus exposed the trick).

Moreover, in this case there was another, subsequent opportunity to bring about such an intervention. Al Rayan Bank made an initial error in terms of the payment type requested in branch. So, it had another chance to engage with Mr R about the payment before it was actually sent from his account. Put simply, at the time the bank called Mr R on 10 October 2019, the £148,066.30 was still entirely within his possession.

Al Rayan Bank has stated that the call recording for this conversation cannot now be produced. So, I cannot say for sure what was and wasn't discussed. Based on what I do know, the bank required Mr R's permission to rekey the payment, especially because there was a corresponding cost for doing so via CHAPS.

He still wanted to go ahead with the payment and was happy to consent to the £15 charge. So, I'm satisfied that he would've been cooperative and was more likely than not to have been open to answering questions about the intended purpose of the payment, and/or the apparent discrepancy between the differing account names and details. In other words, there were two missed opportunities here despite some fairly clear evidence which, to a professional banker, could and should have raised suspicions of a risk of fraud. I am satisfied that, but for those failures, Mr R would not have lost this money.

My conclusions about what is likely to have happened if Al Rayan Bank had asked probing questions are reinforced by the fact that Mr R called M Limited almost straight after the payment had been made. It was at this point that he questioned why he'd been given two different account credentials for the same firm. It is not uncommon for the penny to drop for the ordinary consumer just too late. When they are caught up in the heat of the moment, in the middle of making a large transaction and utterly duped by a clever fraudster, they often don't notice things that later on, with the benefit of hindsight, may seem obvious. That is why it's so important for bankers, as the financial professionals, to take good care and look out for triggers of unusual or uncharacteristic activity.

Mr R says—and I accept—that, reflecting on this meant he started to entertain doubts. But by then it was too late — the funds had already left and were almost immediately removed from the beneficiary bank by the scammers (which meant Al Rayan Bank could not, despite efforts, recover more than £102,045.07 from the payee bank). In light of my conclusions above, it is not necessary in this case to consider whether Al Rayan Bank also exercised enough care and urgency in trying to recover the stolen funds from the payee bank, before they were irretrievably removed by the scammers. But for the avoidance of doubt, there is no evidence that it didn't act with reasonable haste when alerted by Mr R. The fact remains that most scammers manage to remove *all* the funds far more quickly than in this case – so it's fortunate that the losses sustained weren't much higher.

Finally, I have also considered whether Mr R should bear some responsibility by way of contributory negligence. But this wasn't a case of someone foreseeing some sort of harm and taking the risk nevertheless, careless as to the consequences for himself or those to whom he owes a duty of care, e.g. by taking inadequate or no measures to avert it. Mr R simply had no idea that he was being scammed. He received a convincing email purporting to come from his solicitors, and he was expecting this sort of communication to complete his purchase.

As a layman, he had no reason to doubt the email – and wouldn't necessarily know that 11th-hour invoice scams are common. It was not Mr R's fault that he was duped into sending the money astray, and it's clear that he was totally in the dark and simply did not appreciate what he was doing or the consequences of his actions. Accordingly, I am satisfied there was no contributory negligence on this occasion – Mr R was simply the unwitting and blameless victim of a clever fraudster.

My final decision

For the above reasons, I have decided it is fair and reasonable to uphold this complaint about Al Rayan Bank PLC — and I therefore require the bank to:

- Pay Mr and Mrs R the unrecovered £46,021.23 within 28 days of receiving notification of their acceptance of my final decision; plus
- Pay simple interest on that sum at a rate of 8% per year from 10 October 2019 to the date of refund (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R and Mrs R to accept or reject my decision before 1 March 2021.

Matthew Belcher
Ombudsman