DRN-2856416

The complaint

Mr G, on behalf of his company M, complains that Starling Bank Limited won't refund money he lost when he fell victim to a scam.

What happened

In January 2020 Mr G fell victim to a scam.

Based on the submissions of both parties, I understand the background to this complaint to be as follows;

In January 2020 Mr G received a call from somebody saying they were from the fraud department of his internet service provider. The caller said that some suspicious activity had been detected on his IP address, which had left it open to public access, meaning his email, shopping and bank accounts were not secure. Mr G has said the caller seemed to know a lot about him and the accounts he held.

The caller told Mr G the malicious activity on his IP address needed to be cleaned up and to do so it was necessary to carry out checks across a number of online accounts that he held. This included his email address, accounts that he held with online retailers and his bank accounts. The caller told Mr G that even while they were speaking they were tracking his IP address 'live' and could see unauthorised access taking place in a location in London. They told Mr G they knew they were going to hack his accounts, so they stressed to Mr G the importance of having to get things done quickly, to eliminate the risk. But unknown to Mr G at the time, he was actually talking to fraudsters.

The fraudster told Mr G that in order for the malicious activity to be cleared, it was necessary to access his accounts and then come out of the account straight away. Mr G has described how he considered what he was being asked to do as notional activities, aimed at just ensuring his accounts were safe. The fraudsters told Mr G that, where access had been gained illegally, it would have left tags on the account which needed to be cleared, and by carrying out this activity of going into the accounts, it would clear the tags and enable any further suspicious activity to be identified.

The fraudster initially instructed Mr G to check in and out of his email account, and said there was no unusual activity, Mr G has said he was told to do this twice to make sure. At this point Mr G was passed over to another fraudster, who claimed to be a senior advisor for the internet service provider. They told Mr G it was necessary for him to also check his online shopping accounts, talking him through how to do this. Mr G has described that for his online shopping accounts, he was asked to review a purchase and take the transaction right up to the point before payment, to check things were ok. It was Mr G's belief that if he didn't do this his accounts would be at risk and the hackers would be able to use his accounts. The fraudsters told Mr G there was no unusual activity on his shopping accounts.

It is not completely clear when, but at some point during the conversations with the fraudsters, Mr G was struggling to follow their instructions and so they persuaded him that

they would be able to help him more if he allowed them access to his PC, via remote access software, which Mr G agreed to.

Mr G has said the fraudsters had offered their credentials at the beginning of the call, but he asked them for further credentials. In response, the fraudster directed Mr G to a webpage, which he's described as being full of computer code, with white writing on a black background. When there, the fraudsters directed Mr G to a twelve-digit number, which they told Mr G was a 'secure device number', linked to his account with the internet provider. They told Mr G only the provider would know this code, as they said it was unique to Mr G's PC. When the fraudster was able to recite this twelve-digit number, it gave Mr G further comfort that he was talking to his genuine internet provider.

Mr G has said he likened what was happening to a comparable experience he had with a website he uses, whereby he's said whilst it is possible to access this site directly using a standard browser, the link only works if he has already had direct access to it, and if for any reason his browsing history has been erased this access would be denied. Mr G thought this may be because something recognises his IP address as a previous user. Mr G acknowledged that he didn't know if this is factually correct, but in his mind, this experience, led him to believe the fraudsters story had credibility.

Mr G was then told he should check his online bank accounts for any unusual activity. He followed the fraudsters instructions and logged into a personal bank account he holds, with another bank. Again, nothing untoward was found.

Following this, the fraudster asked Mr G if he had any other business banking accounts. Mr G has said he recalled the fraudsters knew about his personal bank account, and that they gave the impression they also knew about his account with Starling. The fraudster told Mr G that this account should be checked too.

Mr G has said that he usually used a tablet for online banking, but was told by the fraudster that in order for a 'clean' to be effective, he should log into his Starling account using his PC. Mr G has described how he attempted to log into his Starling account, on his PC, through the webpage and he requested a number of verification codes to be sent to his mobile, but he didn't receive them. He's said that after several attempts a notification appeared on his tablet that a new payee had been set up. Mr G has said he opened the app on his tablet, which said that a payment had been set up, for £10,000, to a name he didn't recognise.

On receipt of this Mr G has said he told the fraudster about the notification and that it was to a name he didn't recognise. Mr G was asked to authorise this, but as he didn't recognise the name, he told the fraudster he wouldn't. The fraudsters assured Mr G this was all part of checking whether his bank account had been compromised and it was just another way of logging in and out of his account, as he'd done with his email and online shopping accounts. Mr G has also said he asked the fraudsters why it had to be done this way and, while he cannot recall what he was told, he's said it was a credible answer.

The fraudster added that it was a made-up name and was just a procedure to enable the account to be accessed, which was quite safe. The fraudsters offered to change the name to Mr G's name, which they did, and told him that within a few seconds the transactions would show back in his account anyway. Alongside this, the fraudsters continued to tell Mr G that they were tracking a 'live' login on his IP address from another location.

Mr G was reassured when the fraudsters changed the name of the payee to his name and he was told that the funds would be returned within just a few seconds. And, believing it to be genuine, Mr G went ahead and authorised the following payment;

- 21 July 2020 @ 16:36 £10,000

Mr G has said that throughout this interaction he felt under intense pressure to take action to prevent the unauthorised access to his IP address the caller said they were tracking. At one-point Mr G said he would ring off and call back the following day. But the fraudster said although they were meant to be off duty from 5pm, they were willing to stay behind to help Mr G avoid the risk, which Mr G has said he found persuasive.

Soon after, Mr G saw another payment had been set up and the fraudsters told him this needed to be authorised, as they were very close to clearing the malicious activity. Mr G has told us he refused to authorise the payment, even though he says the fraudster was telling him they were close to clearing the malicious activity. They told Mr G they could access his account through their company's main server, which would speed things up and he'd be able to see the refund of the first payment, before authorising the second payment.

Mr G has described how then, after a few minutes a blue screen appeared on his PC, displaying the internet providers name and saying 'main server', quickly followed by a Starling account summary page appearing.

Mr G has said the summary page was the same as he would usually see. He's said it showed that £20,000 had been credited to the account. Seeing this, Mr G believed that the £10,000 he had authorised had been returned to his account, with a further £10,000 being an amount to cover, in advance, the other payment he was being asked to authorise. Convinced that what he was being shown was his genuine Starling account, Mr G went ahead and approved a second payment;

- 21 July 2020 @ 17:26 £10,000

The fraudster then told Mr G the clean-up had not worked and that they were working hand-in-hand with Starling's fraud team and that a further intervention was required. Mr G has said at this point he was apprehensive and so wanted to contact Starling to verify the story. Mr G said he tried to find Starling's contact number online, but was finding it difficult as pages on his PC appeared, then disappeared, which Mr G now believes was down to the fraudsters still having remote access to his PC and being able to see what he was doing. Mr G was eventually able to locate a contact number for Starling and called it, which he did from his landline, while the fraudster was still on the line on his mobile. On talking to Starling, it became clear that Mr G had fallen victim to a scam.

Mr G has said that he doesn't recall seeing any messages or warnings, on either his PC or tablet, when the payments were being made.

Starling contacted the beneficiary bank (the bank where the funds were sent to) to try and recover the money that Mr G had sent, but only £56.66 remained, which was returned to M's account on 3 March 2020.

Mr G complained to Starling and it issued its final response on 5 February 2020. Starling is a signatory of the Lending Standards Board's Contingent Reimbursement Model CRM Code which requires firms to reimburse customers who have been the victims of APP scams like this one in all but a limited number of circumstances. In summary, Starling said that Mr G ignored an effective warning and didn't have a reasonable basis for believing the payment to be genuine.

Unhappy with Starlings response, Mr G then brought the complaint to our service. One of our investigators looked into the complaint. He thought that Mr G hadn't ignored an effective warning. In summary he said this because he didn't consider the warning would have been

impactful in the specific circumstances of this case, as it wasn't specific to what was happening. Our investigator also didn't think it had been established that Mr G didn't have a reasonable basis for believing he wasn't speaking to a genuine employee of his internet provider. In view of this it was our investigator's opinion that Starling should refund M the money it lost, along with interest.

Starling disagreed with our investigator's view. In summary it maintained that it didn't think Mr G had a reasonable basis for belief when making the payments. It said this because Mr G had initially refused to authorise a payment to a payee he didn't know, the fraudster then changed the payee to Mr G. But the account number and sort code didn't change. Starling said if Mr G had checked this he would have been alerted that he was not making the payment to himself. Alongside this, it didn't consider that Mr G making such large payments, could be related to the resolution of a broadband issue he had been contacted about.

Starling added that it didn't agree with our investigator's view that the warnings Mr G had been shown were not impactful. It considered the warnings should have been impactful, considering the customers circumstances, particularly the first warning it showed Mr G, which it said had reference to 'online banking compromise'.

Our investigator considered the points that Starling raised, but they didn't change his position. In summary, he said Mr G hadn't set up the payments himself and was following the instructions of the fraudster – so he didn't consider that Mr G knew the sort code or account number that the payment was going to. He added that the process was following a pattern that had been used to check his other accounts and he had been on the phone for several hours with the fraudsters assisting him. Our investigator added that Mr G's age and knowledge of computers meant there was a disparity in knowledge between both parties. He thought it was reasonable for Mr G to think the service was to help protect him from a cyber-attack. He didn't consider it was fair to say Mr G had no reasonable basis to believe the phone call, considering the sophistication of this particular scam.

Starling responded to say that it believed Mr G would have seen the sort code and account details for the payee, when approving the payment in the app. It didn't agree with our investigator's position that Mr G's age and lack of knowledge about computer's made him more susceptible to the scam. As well as this, it said that the fraudsters had shown a statement with a refund after the payment had been made, and the CRM code states that reasonable basis needs to be established at the time of making the payment.

Our investigator responded to the further points that Starling had made, but his view remained the same. In summary he said the type of fraud Mr G fell victim to was particularly sophisticated, the fraudsters had spent a long time building rapport with Mr G and asking him to carry out a number of tasks to secure his accounts. Given the amount of time the fraudsters had spent building their credibility with Mr G and the apparent threat against the security of his accounts, our investigator considered he had a reasonable basis of belief when he made the payment.

Starling responded. In summary it re-iterated the previous arguments it had made and fundamentally disagreed with our investigator's recommendation.
As agreement couldn't be reached, the complaint has now been passed to me for a 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.

I'm very aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focussed on what I think is the heart of the matter here. If there's something I've not mentioned, it isn't because I've ignored it. I haven't. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service.

In deciding what's fair and reasonable in all the circumstances of a complaint, 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.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account.

However, where the consumer made the payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the consumer even though they authorised the payment. When thinking about what is fair and reasonable in this case, I've considered whether Starling should have reimbursed M in line with the provisions of the CRM Code it has agreed to adhere to, and whether it ought to have done more to protect M from the possibility of financial harm from fraud.

There's no dispute here that Mr G was tricked into making the payments. He feared his personal details had been compromised and that his accounts were at risk if he didn't act quickly. But this alone, wouldn't mean that M is entitled to a refund under the CRM code. It is for Starling to establish that a customer failed to meet a requisite level of care under one or more of the listed exceptions set out in the CRM Code. Those exceptions are:

- The customer ignored an effective warning in relation to the payment being made.

- The customer made the payment without a reasonable basis for believing that: the payee was the person the customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate.

There are further exceptions within the CRM Code, but they do not apply in this case.

I have carefully considered Starling's representations about the warnings it gave and whether Mr G had a reasonable basis for belief. But they do not persuade me that Mr G failed to take the requisite level of care required for the firm to choose not to reimburse under the terms of the CRM Code. I'll explain why;

Effective Warnings

Under the provisions of the CRM Code, as a minimum, an "effective warning" needs to be understandable, clear, timely, impactful and specific. It must also provide information that gives customers a better chance to protect themselves against being defrauded and should include appropriate actions for customers to take to protect themselves from APP scams.

Starling has said Mr G would have seen the following warning(s) when the payment was set up;

Trying to set up a new payee with Online Banking but not seeing the details you have entered on the

website here?

It's likely that the computer or tablet you're using to access the Online Banking has been compromised or you're using a fake version of the Online Banking website.

Stop using the service until you can be sure your device is secure and ensure you always access Online Banking through the link on www.starlingbank.com

Someone asking you to do this?

Starling Bank will never ask you to add a payee or make payments to a safe account. If someone has asked you to, this may be a scam.

Not trying to add a payee to your account?

If you didn't add a new payee yourself with Online Banking, please stop and contact customer service'

Mr G has said he doesn't recall seeing any warnings. I don't doubt he doesn't recall seeing them, particularly given he was being coached by the fraudsters around what steps to take. I think it more likely than not though these warnings were shown. But in any event, even if Mr G had seen the warnings, I'm satisfied that the requirements of the effective warning exception were not met in the circumstances of this case, I'll explain why.

I appreciate that, in displaying this message, Starling took steps to provide Mr G with an effective warning during this payment journey. However, despite this, I'm not persuaded Starling has demonstrated that the warnings it presented met the minimum requirements of an effective warning under the CRM Code.

The CRM Code sets out minimum criteria that a warning must meet to be an 'effective warning'. In very broad terms, it requires that a warning will be capable of countering the typical features of the generic scam type identified during the payment journey. The warning Starling gave does, at least in part, appear directed at the prevention of scams whereby a customer's online banking may have been compromised, where a customer may be asked to set up a new payee or where they may have been asked to move money to a safe account.

But I'm not satisfied this warning did enough to counter the specific type of impersonation scam that Mr G was falling victim to. I don't consider it would bring to life what this type of scam might look or feel like and it doesn't provide any context on how prevalent these types of scams are and how fraudsters are able to disguise themselves and impersonate trusted organisations (such as, but not limited to, a customer's Bank, HMRC, the Police or, as in this case, their Internet Service Provider). I don't think the warning would reasonably have had the desired impact on Mr G's actions to reconsider the payment as a result.
I don't find the warnings sufficient to make the nature of that scam risk apparent to a typical customer (including a microenterprise or charity) or give them enough information to allow the practical assessment of the level of that risk in a specific transaction.

In short, the warning fails to get across in an impactful way what an incipient risk of this type would look like for a customer who hasn't already recognised the scam they may be falling victim to. I'm also mindful that in order for the warning to meet the CRM Code's minimum requirements of an 'effective warning' it should clearly set out the consequences of not taking the suggested steps in the warning. I don't find the warning given makes this

sufficiently clear: for example, setting out that the transaction will be irrevocable, and that if it proves not to be legitimate this will likely mean the funds cannot be recovered. So, I'm not satisfied Starling's warning met the requisite criteria here either.

Overall, I don't consider the warnings given were effective warnings as defined by the CRM Code. It follows that Starling has not established it can fairly apply the exception to reimbursement relating to 'ignoring an effective warning'.

Did Mr G make the payments with a reasonable basis for belief?

I have also carefully thought about Starling's representations about whether Mr G had a reasonable basis for belief. But they do not persuade me to reach a different view. I say that because;

- Mr G had an existing relationship with the Internet Service Provider the fraudsters were impersonating. He held both business and personal accounts with them – so I think it reasonable that he could have considered they would genuinely want to discuss matters with him if his accounts were at risk.

- I don't think Starling has given enough consideration to the fact the fraudster had created an environment where Mr G thought he had to act quickly to protect his accounts from an attack. The convincing nature of these scams can often have a negative effect on a person's thought process and make them take steps that, in the cold light of day, they might not otherwise take.

- Mr G, albeit maybe incorrectly, likened the scenario the fraudsters portrayed, of his IP address being compromised, to something he had experienced. So, I think it is understandable and not unreasonable why he may have thought what was happening seemed plausible.

- The fraudsters took Mr G through a number of steps over a prolonged period of time, keeping him on the phone for several hours and checking numerous accounts. Importantly, in the circumstances of this case, the fraudsters lulled Mr G into a false sense of security by confirming there were no issues with multiple accounts, before targeting his Starling account.

- In particular, the fraudsters bypassed another account Mr G held with a different bank, which they could equally have focused their attention on and sought to gain funds from. Indeed, Mr G has indicated that had they chosen to, it would have been as lucrative for the fraudsters to have defrauded him on that account, as it was for them on his Starling account. But by not doing so, and by reassuring Mr G that things seemed in order, I can understand why it wouldn't have been at the forefront of his mind that the intention of the call was to defraud him.

- In following what he believed were instructions to protect his accounts, I find Mr G did have a reasonable basis for believing the transaction was being made for legitimate purposes, particularly so in that Mr G had been persuaded that he was carrying out a notional activity, that would mean funds showing back in his account, within seconds.

- Mr G has said the fraudsters knew a lot of details about him, including his email and bank accounts that he held. Mr G checked the caller's credentials and they were able to direct him to a webpage and recite a twelve-digit number, that they said only they would know. This persuaded Mr G they were genuine. Which I think is reasonable considering I don't think Mr G would have been aware, that fraudsters would have been able to mockup such a situation.

- Although I acknowledge this would only be relevant for the second payment, the fraudsters were able to mimic a summary page of M's Starling account, showing that credits had been received totaling £20,000. I don't think Mr G would have fairly or reasonably been aware that it was possible for a fraudster to replicate this type of information, in the same way that he was used to seeing from his genuine bank.

- This was a particularly sophisticated scam, where the fraudsters created a number of layers, gained remote access and were able to show Mr G screen images to support their claims of both where they were calling from and that funds were being credited into M's account. I'm not persuaded the average consumer would understand they still might not be talking to a legitimate person, even when the callers are providing complex detail, such as happened here.

Overall, I'm not persuaded Starling has established Mr G didn't have a reasonable basis for belief that he was making a legitimate payment. It follows that I'm not persuaded the exception for reasonable basis for belief applies to the payments Mr G authorised and that Starling can choose not to reimburse M.

Putting things right

Starling should now;

- Refund M the money lost, being £20,000 less any funds that have already been recovered and returned to M and;

- Pay 8% simple interest per annum on that amount from the date it declined M's claim under the CRM Code to the date of settlement.

My final decision

My final decision is that I uphold this complaint against Starling Bank Limited.

Under the rules of the Financial Ombudsman Service, I'm required to ask M to accept or reject my decision before 25 March 2022.

Stephen Wise
Ombudsman