DRN-4208209

The complaint

Mrs G complained against Lycetts Financial Services Limited. To keep things simple I'll refer mainly to "Lycetts".

Mrs G said that Lycetts' actions, inactions, and communication methods enabled a financial fraud to be perpetrated on both her and her spouse. Two separate complaints have been made against the firm, one for each spouse. I'll therefore be issuing two decisions although the two complaints are essentially about the same thing.

This is decision number 2 and covers Mrs G's complaint.

What happened

Mrs and Mr G were directors of their own company. They'd had a professional relationship with Lycetts, their financial adviser, since around 2019. Each financial year Lycetts would email Mrs and Mr G details of the pension contributions both of them could make before the tax year end and my understanding is that these payments would be made from the company they were directors of. Their company had a bank account with a well-known 'high street bank'.

Typically, the email Lycetts sent would carry an attachment which included financial illustrations, confirmation letters and bank details so she and Mr G could send the pension contributions to Lycetts to be invested on their behalf. We know, for example that this process had been used in 2020 when a large sum was sent to the firm for investing, and again in 2021 when they invested another large amount using the same communication arrangements. This all worked without incident and monies were duly paid into the correct pensions.

For the matters now complained about, it seems Lycetts sent a legitimate email on 23 March 2022 in line with the established process. But neither Mrs nor Mr G probably ever saw this email from Lycetts because it seems a fraudster was able to prevent them from seeing it. The fraudster was able to use the legitimate Lycetts email to create a convincing forgery – a false email pretending to be from Lycetts. This showed the Lycetts employee's email address at the head, complete with a display name which matched details evidently familiar to Mrs and Mr G.

The fraudster, by using this contrived email, was then able to 'discuss' the pension transfers with Mr G, who it seems dealt with his and Mrs G's financial affairs in this regard, and he subsequently sent a total of £97,053 over three payments (as requested) to the fraudster who was impersonating Lycetts. The fraudster replied to say that the payment had been received.

Nevertheless, we now know that at no point was either Mrs or Mr G ever dealing directly and legitimately with Lycetts over the course of these communications. Instead, it seems these communications were with the person defrauding them, with Lycetts at that point being completely unaware of what was happening.

The fraud wasn't uncovered until April 2022. Mr G has complained on his and Mrs G's behalf to the relevant high street bank which the transfers had passed through. I think it's fair to say that the banking sector's approach to these types of payment fraud has evolved over recent years. And so bearing this in mind, the bank in question admitted it probably shared some responsibility for what happened. However, to be clear, it also said Mrs and Mr G bore significant responsibility too because the likely scenario here is that Mrs and Mr G's email account had been the source of the compromise. The bank agreed to pay their company account a total of £20,005.17 which comprised of £20,000 plus a very small amount of funds it recovered. I understand the bank later made a further cash offer in addition to this sum.

When Mrs and Mr G brought a complaint to Lycetts, during its investigation Lycetts asked an independent consultancy to look into what happened and mainly at Lycetts own IT system. This consultancy concluded that Lycetts IT system had *not* been hacked.

Mrs and Mr G also contracted a specialist IT company to look at their company email. Mrs and Mr G were told there was no direct evidence that their email address had been compromised. Lycetts didn't uphold the complaint.

Mrs and Mr G have brought their complaint to the Financial Ombudsman Service. One of our investigators looked into the case and said they thought it should be upheld. And they thought Lycetts should pay Mrs and Mr G some redress.

Lycetts disagreed with this and said that both Mrs and Mr G and their bank were liable. Due to that investigator leaving the Service and the case being identified for a review, another investigator was asked to look at the complaint; and that second investigator came to a different conclusion. They said Lycetts wasn't responsible for the loss and said the complaint against it should not be upheld. Mrs G didn't agree with this.

The complaint has been passed to me for a final decision as the parties can't agree. And to be clear, I'm only considering the complaint specifically against Lycetts here. I can see Mrs and Mr G have already received responses about their bank and its liability and so I won't be covering that aspect in this 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've used all the information we have to consider whether Lycetts should pay any redress in this case. I've also taken into account relevant law and regulations, regulator's rules, guidance and standards and codes of practice, and what I consider to have been good industry practice at the time. I have further considered the contingent reimbursement model operated by various financial businesses.

I've considered the very detailed responses I've had back from Mrs and Mr G. I'd like to thank them for taking the time to set out their grievances in a very comprehensive and clear fashion. I can also confirm, in response to a recent email from Mr G, that I have considered everything that's been said, including what our first investigator thought should happen.

But having done all this, I am very sorry to disappoint Mrs G. I regret that I am not upholding this complaint.

Introductory issues

I'd like to assure all the parties that I do understand the terrible fraud that has evidently taken place here and I certainly understand that Mrs G wants someone to be held responsible. However, in my view, our second investigator has carried out a very comprehensive analysis of what has taken place. More so, I think his conclusions were based, rightly, on the evidence we have in this case and also the consistent approach we take to these situations. I'm afraid my conclusions don't differ from his.

As a reminder, the complaint I'm dealing with here is against Lycetts, not the bank. As I've said, Mrs and Mr G brought a complaint directly to their bank which produced the partial offer of redress which I've mentioned above.

I think it's also possible to become intrenched in very technical areas of IT in this case. However, the crux of the matter here is relatively simple. Given the bank's responsibility has already been addressed elsewhere – and the details of the on-line journey Mrs and / or Mr G took to transfer the money from their web-based banking account – the remaining liabilities, in my view, relate mainly to which email account was unlawfully used. It is on these issues that my Decision focusses. And I'm afraid I respectfully disagree with Mrs and Mr G about *"the narrow issue of who was hacked being irrelevant"* in this case. This is simply because it would be unfair of me to hold Lycett's responsible for something that happened to another party and in which it had no hand.

Mrs and Mr G also say Lycetts' role was *"to deal with multiple retail clients whose IT security cannot be vouched for"*, the implication being that lax IT security and communication practices by the firm was the cause of Mrs and Mr G's loss. Again, I think it would only be fair of me to consider this had those issues been the fundamental enablers of what happened here.

What likely happened?

As I've said, each of the parties contracted an IT specialist to carry out examinations of both Lycetts' and Mrs and Mr G's email systems. But whilst they do differ slightly in their conclusions, neither found any evidence that Lycetts' systems were hacked by an unauthorised actor, or that the fraudulent email was sent via its servers.

In my view, what has essentially taken place is something termed "spoofing". I'm afraid it is very difficult to stop email spoofing because the Simple Mail Transfer Protocol (SMTP), which our investigator explained, is the foundation for sending emails. This doesn't require or mandate any authentication process. There are some additional countermeasures which have been developed to counter email spoofing, however the success rate will depend entirely on whether Mrs and Mr G's company email service platform implemented them. Typically, additional authentication can be viewed by some as more time consuming and / or onerous and so in my experience this is rarely implemented.

I agree that with the benefit of hindsight Lycetts, a professional firm, could have been somewhat commercially naive in sending sensitive information about financial matters in the way it had been doing for several years, especially where large amounts of money were involved. Nonetheless, its role was to have a mutually productive business relationship with clients, and it seems the previous method of communication was trusted and accepted between the parties and indeed, previously successful.

For me to find Lycetts being responsible for this loss, I would need to think that its email to Mrs and Mr G's company requesting this was intercepted at source by the fraudster. I would need to believe it was not due to a breach *after* it had left Lycetts account and had arrived at Mrs and Mr G's company email. There is insufficient evidence to support this theory and I can see that *authentic* emails from Lycetts were sent from a UK based provider, whilst the

fraudulent ones came from a server overseas. In my view this demonstrates a relationship – albeit an unlawful one – directly between the fraudster and Mrs and Mr G.

So, having considered all the transactional evidence, the approach I must take is to think about what is *more likely* to have happened. And the far more likely scenario is that this fraud was only able to be perpetrated due to Mrs and Mr G's email account being compromised at their end. I think the evidence is persuasive that someone accessed their email account and then used the information they found therein to establish a false relationship as a prelude to building up a picture of their financial affairs and then carrying out a criminal offence. I am afraid this is a much more common fraud trend we do tend to see, where a criminal actor gained access to Mrs and Mr G's email and was able to use this access to create a convincing forgery. It was then made possible to delete the original *genuine* email from Lycetts about annual pension contributions, to an extent Mrs and Mr G were unaware of its existence. This would account for how the fraudster was able to know which employee name from Lycetts they should use in order to seem plausible.

In my view, it's very unlikely that Lycetts emails system was ever breached in the way Mrs and Mr G allege. I therefore agree with what our second investigator said – that there's no persuasive evidence that Lycett's genuine email could, in simple terms, have been 'plucked out of the air' prior to it reaching Mrs and Mr G and / or their company.

Other issues

Mrs and Mr G make a number of other points relating mainly to how Lycetts conducts its business with clients. These include, although are not limited to, the following:

- That Lycetts hadn't implemented a DMARC configuration (which helps confirm the 'header' on the email sender is trustworthy)
- That it's cyber / IT security policy was poor
- That secure communication with its clients was lacking, and
- It had response / governance failures

However, if I were to hold Lycetts responsible for the loss in this case based on these issues, I'd be holding it to account for things which are widespread and practiced by thousands of companies throughout the United Kingdom. There's simply no evidence that the lack of a DMARC configuration at Lycetts' end contributed in any way to this issue. And the issues of having cyber / IT security policy refers, for example, to *having in place up-to-date policies and procedures appropriate to its business which must be readily accessible, effective and understood by all relevant staff;* there's no evidence this wasn't the case. Similarly with secure communications, there's no requirements here which I'm aware that Lycetts failed on. And, 'Governance' is a very wide issue which again, I can find no failures or that this impacted upon this unfortunate case.

Summary

In my view, all these things mean Lycetts cannot be fairly or reasonably held responsible for the loss in this case. I've noted that Mrs and Mr G part-pursued the (on-line) banking issues as cause for a complaint but as I understand it, this route has now closed due to time barring rules. In any event, my Decision here cannot relate to that separate matter.

For the complaint against Lycetts, I have thoroughly read everything said about how its' procedures could have been much better. And of course, I urge Lycetts to learn important lessons for their on-line dealings with clients in the future.

I also certainly wouldn't wish to imply in any way that Mrs and Mr G were responsible for what happened, but I do think it was their email system which was compromised. Therefore, even if Lycetts could have acted differently in its communications with clients, I can't hold it responsible for the fraud perpetrated on Mrs and Mr G.

Once again, I'm very sorry to disappoint them.

My final decision

I do not uphold this complaint or require Lycetts Financial Services Limited to do anything more.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs G to accept or reject my decision before 31 March 2024.

Michael Campbell
Ombudsman