DRN-5195214

The complaint

The members of Mill Road Group SIPP complain that Westerby Trustee Services Limited acted on fraudulent payment instructions. Some funds were returned by the receiving bank, but the SIPP members have still suffered a considerable financial loss.

The complaint has been brought by one of the members of the Mill Road Group SIPP ("Mrs P1") on behalf of them all.

What happened

The Mill Road Group SIPP ("MRGS") is made up of six member trustees (three married couples) Mr and Mrs P1, Mr and Mrs P2, and Mr and Mrs P3, and they hold their pension savings in a Self-Invested Personal Pension ("SIPP"). They use the assets within their SIPP to develop and renovate properties. Westerby Trustee Services Limited ("Westerby") is the scheme trustee.

MRGS has a current account held with a bank I'll refer to as "M", and the signing mandate requires any two of the member trustees plus a signatory from Westerby to authorise payments. At the relevant time M wasn't able to offer "*Confirmation of Payee (Requester)*" checks to confirm to customers paying funds to another bank that the sort code and account number matches the beneficiary they wish to pay.

In 2022 MRGS was developing a commercial property and had engaged a building company to carry out the refurbishment. The building company claimed payment for the work done in instalments, by submitting invoices to the project managers ("JE"). JE would verify the work had been completed satisfactorily and then forward the invoices to an individual I'll refer to as "Mr K" who had been appointed by MRGS to handle the payment administration and *"keep track of the approvals for the SIPP properties*". Mr K would liaise with Westerby to create the proforma payment instructions which would be passed to MRGS for authorisation by two of the members in accordance with the signing mandate. Once approved Westerby would submit the signed instructions to M for payment via the electronic BACS system. This process had worked successfully for a number of years for this and previous projects.

On 18 November 2022 the building company issued two genuine invoices (for instalments nine and ten) for payment to JE, which approved the invoices and emailed them to Mr K to arrange payment. On 25 November 2022 Mr K commenced the usual payment process by asking Westerby to raise a BACS sheet for the invoices. An hour later Mr K told Westerby to ignore his previous email as he'd been told the building company's bank details were incorrect, and he'd forward revised instructions when he received them.
Mr K received these instructions by email from an account purporting to be from the main contact Mr N at the project managers "JE", but he didn't notice any discrepancy with Mr N's email address.

On 27 November 2022 Mr K received revised invoices with amended bank details which he passed to Westerby to raise the BACS form. The following day Westerby sent the payment instructions to Mr K to arrange for authorisation. Two members of MGRS signed the

instructions in accordance with the mandate on 1 December 2022, which were then forwarded by Mr K to Westerby for countersigning. Westerby submitted the signed instructions to M on 2 December 2022 for payment. In line with its process for handling high value payments M phoned Westerby asking them to confirm the payments which they did, on the basis they were expected and in line with other instalments for the project. So on 2 December 2022 M made the payments. totalling around £148,288 to the bank details quoted on the revised invoices.

The fraud came to light on 4 December when JE chased the payment on behalf of the building firm, and the fraudster posing as "Mr A" the main contact at the building firm confirmed (by email) it had been received. This prompted JE to phone the genuine Mr A, and they subsequently discovered their email accounts had been hacked.

On 7 December 2022 the receiving bank notified M that it suspected the funds were the proceeds of a fraud. And on 14 December 2022 Mr K called Westerby to let them know they'd been tricked into paying fake invoices identical to the originals apart from the bank details. The matter was reported to the police and Action Fraud, and a full investigation was carried out by the relevant parties, but the full funds could not be recovered. Around £93,026 has been returned to M by the receiving bank, but as the building company still needed to be paid, MGRS has incurred a loss of £55,352.

MGRS has also complained to bank M regarding its role in the transaction which is being dealt with separately.

In June 2023 Mrs P1 on behalf of the members of MRGS complained to Westerby that it had failed to prevent the fraud. Westerby responded in August 2023 saying it had acted on the fraudulent instructions in good faith but offered £750 for the distress and inconvenience caused. This was not accepted by the members of MRGS.

On further consideration, Westerby proposed sharing responsibility and the resulting financial loss between all the parties involved. So Westerby offered to pay MRGS £11,700.40, being one fifth of the loss. This was rejected, and Mrs P1 brought the complaint to this service on behalf of all the members, holding Westerby liable for the full loss.

Provisional decision

I issued a provisional decision in November 2024 setting out my initial thoughts and allowing the parties a final opportunity to comment. I've set out a summary of my provisional findings below.

> *I was sorry to hear MRGS has been the victim of a sophisticated fraud, which is understandably upsetting for the members. It succeeded because fraudsters were able to hack the email accounts of the builders and project managers, intercept the genuine invoices and persuade Mr K not to pay them, but to wait for replacements containing the fraudster's bank account details. And because at the time bank M wasn't able to check the sort code and account number matched the payee's name, which would've revealed they didn't relate to the building firm. Westerby's own emails weren't hacked, and there's no evidence Westerby's systems were compromised, or that it was duped by the fraudsters.*
>
> *So the fraudsters are the guilty parties here. And while MRGS is out of pocket, it doesn't necessarily follow it should expect to recover its total loss from Westerby, just because they are the only FCA regulated business involved in the transaction, (apart from bank M whose role has been considered separately). This decision only concerns the actions of Westerby, but in order to set out the sequence of events I have referred to several other parties involved in the transaction, although I've made no findings on their actions.*

I considered Westerby's role and responsibilities as the SIPP trustee. These require it to ensure the proper running of the scheme including compliance with HMRC rules, invest the assets, produce annual valuation statements, and handle aspects such as the collection of contributions and distribution of benefits.

The Master Trust Deed which sets out the rules of the scheme is silent on how payments on behalf of Group SIPPs will be handled, as is the Deed of Appointment and Supplemental Deed from 2012. I've then looked at the Schedule of SIPP Fees from July 2022 which would have applied at the relevant time. This sets out the services Westerby provides in relation to establishing and administering a SIPP. The charges are set out in sections setting up the SIPP, contributions, purchasing assets, taking benefits investing in property and non-standard assets and transfers and winding-up. One of the responsibilities under "general administration" is the operation of the SIPP bank account, but there's nothing specified about the process for handling large value payments (or any payments).

So in the absence of a specific term in the contract which covers this, I've relied on the law, regulatory rules, guidance and codes of practice any firm is required to follow, as set out in the Financial Conduct Authority handbook. Of particular relevance are the Principles for Business ("PRIN") specifically 2.1.1R principles 2, 6 and 10 as follows:

Principle 2 – a firm must conduct its business with due skill, care and diligence
Principle 6 – a firm must pay due regard to the interests of its customers and treat them fairly
Principle 10 – a firm must arrange adequate protection for its clients' assets when it is responsible for them.

I didn't think Westrby was solely responsible for Westerby's assets in the way suggested in PRIN 10. But Westerby played a role in the overall invoice payment process, so was required to exercise due skill, care and diligence, and treat the members of the SIPP fairly.

M will only accept payment instructions from a SIPP bank account from the SIPP trustee (Westerby), not from the members direct or another third party such as an IFA. Meaning neither MRGS or Mr K could submit payment instructions to M, they had to go via Westerby to create the BACS sheet. So the established process to pay the building firm's invoices involved a number of steps prior to reaching Westerby. The invoices were first approved by the project managers JE then passed to Mr K a trusted family member appointed by MRGS as administrative support. Finally they were reviewed and signed by two members of MGRS.
Westerby was expected to carry out a number of checks prior to submitting the payment instructions to M:

- ***Were the payments expected and were they received in the usual way****? These were the next two instalments of an ongoing project, and Mr K had let them know to expect revised instructions. They'd been received in the usual way, by email from Mr K which was an established method of communication.*
- ***Do these payments represent out of character activity for the SIPP****? These were instalments nine and ten there had previously been eight similar payments within ten months, and Mr K (and previously JE) had confirmed they were funds due to for refurbishment work carried out.*

They were signed by two authorised signatories of MRGS, and the SIPP bank account held sufficient funds to make the payments with no concerns about the source of those funds.

- *Westerby is a mandatory counter-signatory to all payment instructions, but I think the aim of this fraud prevention measure is to disrupt the fraudulent or unsuitable transfer of pension assets, rather than the payment of invoices related to a refurbishment project.*

The building firm's invoices include their account details with a high street bank. The payment instructions created by Westerby included the updated bank details taken by Mr K from the replacement invoices. At the relevant time M didn't operate "confirmation of payee" checks which weren't mandatory. Had M been able to check the revised details it would've been apparent that the quoted bank details didn't match an account in the name of the building firm, and that the sort code related to an Electronic Money Institution rather than a high street bank.

*Without those checks, I thought the fraud could only have been prevented if the building contractors had been asked to confirm they had changed their bank details, which would've revealed the intercepted emails arising from the accounts being hacked. But Westerby had no relationship with the building contractors and had received the instructions from Mr K in the usual method and format, having previously been signed off by the project managers. MRGS believes that when Mr K informed Westerby the building company's bank details had changed they should've considered the possibility of invoice interception fraud. But I thought it was reasonable for Westerby to rely on the account details it had been provided with, as Mr K hadn't disclosed that an hour after the first email, he'd received a second email unexpectedly telling him the builders had changed their bank. Instead he informed Westerby he'd "just been **told** the bank details are **incorrect**" (my bold emphasis).*

The possibility of invoice interception fraud may have been triggered if Mr K had said he'd unexpectedly received the new bank details by email. But perhaps unintentionally I think he gave the impression he'd received the information verbally, direct from a contact at the building company, rather than by email. And the description of the bank details being "incorrect" may simply have suggested a mis-type in the original invoice. Based on what it knew at the time, I saw no reason Westerby should've s been aware of any "red flag" fraud indicators.

In its complaint investigation Westerby denied receiving a confirmation call from M and said the only contact had been by email on 7 December 2022, three working days after the payments were made. I clarified that M actually had phoned Westerby to confirm the payments, in line with M's standard procedure for high value payments (over £10,000) once the signatures had been checked to the mandate, it wasn't due to any concerns about these payments in particular. So I said it would've been routine for Westerby to receive calls from M in relation to payments from the MRGS account, and only payments over £250,000 were confirmed direct with MRGS. The limit was previously lower at £100,000, but that still wouldn't have caught these two payments which were £61,560 and just over £86,728.

I clarified that the 7 December 2022 email mentioned by Westerby and our investigator arose when the receiving bank alerted M to the possibility the funds received by its customer were the proceeds of fraud. It was sent at 17.37 from M's "partnership support team" advising Westerby that "2 payments have been flagged …." and asking them to check they were genuine. It wasn't from M's fraud department, nor does it mention suspected fraud, and in any case it was after the payments had been made.

I'd listened to the call from M to Westerby on 2 December 2022 to verify the payments. For each payment the agent at Westerby confirms the amount, the SIPP account (held with M) to be debited, the payee being the building contractors, the (replacement) sort code and account number and the reference number. Then the agent from M reads from a script as follows "Can you confirm you have validated the beneficiary account details with the member verbally and/or independently and that the details on the form are one hundred per cent correct?" to which Westerby replied "We've checked them, yes". I said as Westerby hadn't done that, it shouldn't have responded as it did. But though Westerby shouldn't have confirmed it had "verbally" verified the payments with the SIPP members, it may have considered the details had been verified "independently" (by Mr K) as being "one hundred per cent correct".

So I thought carefully about what was likely to have happened if Westerby had answered that question correctly, by explaining the instructions were received, as usual, not direct from MRGS but from a trusted third party (Mr K) appointed by the members. Clause 14 of the 2012 Supplemental Deed allows the SIPP members to appoint an agent (such as Mr K) to handle matters on their behalf. The signed "same day" payment instructions were emailed from Westerby to M at 12.56 on Friday 2 December 2022.

It's not clear from the recording what time M called Westerby, but the payments were sent at 4.32pm and 4.34pm. Any delay in the verification process may have meant them being held over to the next working day, Monday 5 December. I'd seen that on 30 November "Mr A" from the building firm had emailed Mr K to chase progress. A sense of urgency can be a fraud indicator, but equally firms are entitled to chase up late payments, and the invoices were dated 25 November, so were already overdue.

Even if Westerby had attempted to verify the payments they wouldn't have gone direct to the building firm with which they had no relationship. They probably could have contacted one of the members of MRGS but given the time pressure approaching close of business on a Friday afternoon, I thought it likely they would still have been referred to Mr K, as he handled the payment administration on their behalf. He had seen the invoices which the members hadn't, and he had access to the building contractors' bank details which they wouldn't necessarily have had to hand. And I thought Mr K is likely to have confirmed the bank details were correct as he had no reason to suspect the email he received from the project managers, apparently copying in "Mr A" from the building contractors wasn't genuine.

I said the updated bank details appeared on the instructions signed by two members of MRGS, and it wasn't clear if Mr K had told them the building firm's bank details had changed. It also wasn't clear if the signatories noticed the change, but even if they had, given they knew the instructions had been submitted to Westerby by Mr K, who was closely involved in the project and who they trusted, I think it's likely they would've assumed the information came from a reliable source and not questioned it further. If they checked anything, it was probably limited to the amount being in line with what they were expecting to pay for instalments nine and ten.

M's email flagging the payments was prompted by the receiving bank and came days after the payments had been made. Having carefully considered the sequence of events, and based on what Westerby knew at the time, I can't reasonably say they should've alerted Mr K or MRGS to the possibility this was invoice interception fraud.

Fraud prevention measures only work if all parties are vigilant. So even though the call from M to Westerby was routine rather than due to any particular concerns

Westerby shouldn't have said it had verified the payment details when it hadn't. But the fraud was successful due to a chain of events – the hacking of the building company and project managers' emails, Mr K not realising he'd been contacted by an imposter, and taking what he was told at face value, and the signatories of MRGS signing the payment instructions without noticing or querying the changed bank details. Westeby says it acted in good faith, had no way to independently verify the building company's account details, and the instructions had been confirmed by JE and Mr K. Even if Westerby had queried the change, I thought it more likely than not they would have been referred back to Mr K rather than MRGS, and this would not have prevented the fraud. Just because Westerby has subsequently tightened its procedures, it doesn't follow that its actions at the time were unreasonable.

So while I had sympathy for MRGS being victim to a fraud, I didn't think it was fair to hold Westerby responsible for their entire loss. They were one of the parties involved in the transactions whose combined actions enabled the fraud to succeed. So on that basis I found their offer to reimburse one fifth of the loss to be fair and reasonable.

Responses to the provisional decision

Westerby accepted it and had nothing further to add.

MRGS didn't accept, and their representatives made the following points (in summary)

- The confusion around whether the payments were checked by phone or email is evidence Westerby wasn't transparent from the outset. And failing to acknowledge the existence of a phone call was a deliberate attempt to mislead the complaint investigation. And it's an unsafe assumption that the phone call from M to Westerby was "*routine*" rather than an indicator that fraud was suspected.

- This complaint should be viewed in the light of the prevalence of "APP" (authorised push payment) fraud which presents a significant financial risk.

- Westerby (not Mr K) was the gatekeeper in relation to this payment and the interface with the paying bank ("M"). Its role was to protect trust assets.

- The script read by the agent from M draws the other party's attention to the possibility the payment might not be genuine, which is not routine. And only Westerby received such a warning.

- Westerby's "*misleading*" response to M's question was the "*direct and proximate cause of the loss"* meaning it must be the responsible party.

- Had Westerby disclosed to M that the bank details had been changed, the payments would've been put on hold pending the required confirmation. Or they would have proceeded on the basis that Westerby accepted the risk of the payments not being genuine.

- To verify the payments, Westerby would've gone back to Mr K who would then have telephoned JE or Mr A at the builders and the fraud would've "*unquestionably*" been discovered and prevented.

- A conversation with Mr K would've involved alerting him to the possibility of APP fraud and the "*red flag risk factors"* and the necessity of speaking direct to JE or the building company. These risk factors being emails received one hour apart, the bank

details being fundamentally changed rather than a digit being mistyped, and all communication being by email – all indicators of APP.

- It's been accepted that Mr K's email account was not hacked, but Westerby couldn't be sure his emails had not been compromised. Proper "*independent*" verification of the payment instructions would've required Westerby to bypass Mr K and make direct contact with JE or the builders.

- Westerby alone was asked by M to confirm the payments, and that confirmation gave M comfort to make the payments. So it's not realistic or appropriate to apportion blame equally to all parties.

- The fair outcome is for Westerby to reimburse MRGS for the entire loss.

I also obtained copies of the fraudulent emails, and asked MRGS for details of what checks they undertook prior to signing payment instructions

So I'm now in a position to issue the final 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.

MRGS has placed a lot of weight on Westerby's initial denial a call took place from M prior to the payments being made. This was an error which arose because the call from M was made to check a number of payments to be made from different pension accounts, not just MRGS. Having listened to the call, one agent from M asked Westerby about unrelated payments from another account, and then once those have been dealt with, hands over to a colleague handling the MRGS payments. As the payments relating to MRGS weren't the first or only payments discussed in the call, it wasn't readily located when the call was searched for. I find this explanation plausible, and while this may have hampered the complaint investigation after the fact, I don't think it was a deliberate attempt to mislead, nor was it a factor in the fraud itself, so I don't draw negative conclusions from this.

Also M confirmed (in relation to the linked complaint) that making a call to Westerby as the SIPP trustee to verify the payments was standard procedure for high value payments from all pension accounts (SIPPs and SSASs). So it was routine for the script to be read out for any payment from a pension account over £10,000. Although such a step is intended as a fraud prevention measure, I'm satisfied M had no particular concerns about those payments, and it wasn't triggered due to the change of bank details. M would only call a member trustee (in this case MRGS) if the payment value exceeded £250,000 (previously £100,000). M has provided evidence to show calls were made to MRGS in relation to payments of £322,739 and £731,310. But even if the limit had remained at £100,000 this wouldn't have caught the fraudulent payments as both were under this limit.

I agree with the representatives of MRGS that the fraud would've been discovered had someone called either the building contractors to check if they had changed banks, or the project managers JE to ask if they had submitted replacement invoices. But a call like that would only take place had suspicions been raised. APP fraud where the customer is tricked into authorising a fraudulent payment is increasingly prevalent. But I don't think it's reasonable to expect Westerby to have identified these payments as potentially fraudulent due to invoice interception, based on the information it had at the time.

The established process for making payments by instalments to the building contractors for this project had worked successfully on eight previous occasions. The invoices were raised by the building contractors and approved by the project managers before being sent to Mr K who liaised with Westerby to raise the BACS instructions, which were then authorised by two signatories from MRGS. Generally only Mr K had direct contact with the building firm and the project managers, Westerby's day to day relationship was with Mr K, as appointed by the members.

The representatives of MRGS point to several "*risk factors*" as indicators of APP fraud - the conflicting emails received one hour apart, the bank details being fundamentally changed rather than a digit being mistyped, and all communication being by email.

So I've reviewed the genuine email sent on 18 November 2022 from Mr N, the main contact at JE the project managers. The content is brief but professional, attaching and authorising the payment of invoices nine and ten. As well as Mr K, it was addressed to Mr U a contact at the local authority, copying in Mr A the main contact at the building contractors, Mr N's genuine email address is as follows "[*Mr N's first name*]@[*full name of building contractors*].**co.uk**" (my bold emphasis).

I compared this with the fraudulent emails sent to Mr K on 25 November 2022 notifying him the builders had changed bank accounts. These originated from a slightly different email address "[*Mr N's first name*].[*full name of project managers*].co.uk**@outlook.com**". This email was not seen by Westerby, and Mr K couldn't have noticed, or appreciate the significance of it originating from an Outlook account, rather than JE's genuine company email address.

The first fraudulent email apparently from Mr N was sent at 13.16 on 25 November 2022, and read as follows: "*I have just got a call from [name of building contractor] that their bank details has (sic) been changed since 20th of November, please contact your account to hold as he has instructed their account to amend the invoices and i (sic) will forward it to you soon sorry for not informing you prior to sending the invoices, apologies for the inconvenience caused. Please confirm the payment process has been stopped"*. It was signed off with Mr N's genuine details, presumably taken from the intercepted email.

This email was sent to Mr K, as well as what appear to be the genuine email addresses of Mr A at the building contractors, Mr U at the local authority, and "H", one of the members of MRGS. Then at 13.55 on the same day, another email was sent from the same Outlook account to the same email addresses including H at MRGS, enclosing the replacement (fraudulent) invoices.

Apart from the original genuine submission of invoices nine and ten, I'm not familiar with Mr N's usual communication style. But in my view, the written English in the email on 25 November is not of a professional standard commensurate with someone of his qualifications and seniority, and that together with the changed email address can be a fraud indicator. So if Westerby had been party to this exchange I'd have expected it to have considered the possibility of fraud, and alerted Mr K and MRGS.
But Westerby didn't see the fraudulent emails until they were disclosed as part of the complaint investigation, but they were seen by both Mr K and H from MRGS. From the signing mandate, it doesn't appear H was one of the two MRGS signatories who authorised the fraudulent payment instructions, which MRGS has said could be whoever was available. MRGS has also confirmed when authorising invoices, they only review the certificates to ensure the scope of work was correctly recorded, they rely on Westerby for the "*mechanics*" of the payments. But there was an opportunity for Mr K or H to have shared with their fellow MRGS members that the builders had unexpectedly changed banks on 20 November, but

that JE the project managers had only been notified on 25 November, a week after the invoices had been approved.

Further, the email trail Mr K sent Westerby with the replacement invoices nine and ten, included the original, genuine email from Mr N the director at JE (showing his genuine email address), copying in Mr A the director of the building firm, and Mr U from the local authority. Westerby did not see the email purporting to be from Mr N from the Outlook account until after the fraud had taken place. And Mr K didn't tell Westerby he'd received slightly garbled email instructions from "Mr N" asking him not to pay the original invoices but to wait for replacements. Instead Mr K said he'd been "*told"* the building company's bank details were "*incorrect*". So I remain of the view Westerby wasn't made aware of any particular indicators of invoice interception fraud.

I've already said that Westerby shouldn't have confirmed to M it had "*checked them*" when asked about the payment details. But I think it could have considered the details had been "*independently verified*", given they'd passed through the project managers JE, Mr K as MRGS's agent, and two members of MRGS who signed the payment instructions clearly showing the substituted sort code and account number on 1 December 2022, prior to them being countersigned by Westerby the following day.

I'm not persuaded it's more likely than not that if prompted by a routine verification call, Westerby had gone back to Mr K asking him to confirm the payments, he would "*unquestionably*" have telephoned either the project managers JE or the building company to confirm the instructions were genuine. After all Mr K was under the impression he'd received the amended instructions from his usual contacts in the usual way. He hadn't thought the change of bank details was suspicious and hadn't noticed the discrepancy in the email address or the less than professional content of the email. So I can't reasonably say he'd have done more than compare the details on the replacement invoices to the payment instructions submitted to Westerby, which had been signed by two members of MRGS on whose behalf he was acting, and confirmed they were correct.

I don't consider it reasonable to expect Westerby to verify the payments with the building company or project managers direct. This wasn't the established process for the previous payments, and instalments nine and ten were not out of character for the project. Westerby's relationship was with the MRGS members, who had appointed Mr K to act on their behalf. Westerby had no concerns about Mr K or his abilities, and I don't think MRGS would've expected Westerby to bypass a trusted family member who had a key role in the project team.

Equally I don't think it was necessary for Westerby to have told M the payee's bank details had changed, and it may not have been passed on within Westerby, from "J" the pensions administrator who dealt with Mr K to the agent who handled the call from M. I bear in mind the time pressure approaching close of play on a Friday afternoon, so any steps to verify the payments is likely to result in them being held over until Monday. And further delays to the payment of overdue invoices may have jeopardised MRGS's relationship with the building contractors.

M required payment instructions from pension accounts to come from Westerby, not the members, and its role is to protect the trust assets. But that is also the responsibility of the MRGS signatories, which is why there are two, who signed off high value payment instructions without noticing or querying the changed bank details.

Much of what has been said about Westerby's actions or omissions is with hindsight. The fraud was successful due to hacked email systems at third parties (the building contractors and project managers), not at Westerby whose communications weren't compromised. It's

not reasonable to expect Westerby to suspect Mr K's email may have been compromised, prior to the hack coming to light. Westerby wasn't copied in to the emails showing the fraudulent email address for Mr N, the only emails Westerby received showed Mr N's genuine email address and the original content, and included other parties to the project. Westerby could only have taken steps to prevent the fraud had it been made aware of the potential "*red flag*" indicators, but those who had access to that information didn't pass it on to Westerby. I cannot hold Westerby responsible for not acting on information it didn't have.

Having given the matter very careful consideration, I'm not persuaded based on what they knew at the time, that if Westerby had referred the payments back to Mr K or answered the question differently confirming the payments had been "*independently verified*" the fraud would've been prevented. As I can't say it's more likely than not this would've resulted in direct telephone contact with either the builders or JE.

So I remain of the view that it would be unfair to hold Westerby solely responsible for MRGS's financial loss, and its offer to refund a proportion of the loss was fair and reasonable.

Putting things right

Westerby Trustee Services Limited has made an offer of £11,070.40 to settle the complaint, and I think this is fair in all the circumstances for the reasons set out above. So my decision is Westerby Trustee Services Limited should pay £11,070.40.

Compensation must be paid within 28 days of the date on which Westerby is notified MRGS has accepted the final decision. If the compensation is paid later than this, Westerby must also pay interest on the compensation from the date of my final decision to the date of payment at 8% simple per year.

My final decision

I uphold this complaint. Westerby Trustee Services Limited should put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask M to accept or reject my decision before 30 April 2025.

Sarah Milne
Ombudsman