DRN-2771930

The complaint

Mr S complains that James Hay Administration Company Ltd trading as James Hay Partnership ("James Hay") hasn't agreed to fully refund fraudulent payments from his Self-invested personal pension (SIPP).

What happened

Mr S has had a SIPP with James Hay since 2003. He takes a regular monthly income of around £2,000 which is paid into his account with bank "S". Mr S has periodic reviews with his financial advisor (not from James Hay) regarding his investment strategy.

In June 2019 James Hay received an email apparently from Mr S asking to set up online access to his SIPP. As part of its security procedure James Hay wrote to Mr S at his home address with a code to set up the online access. This letter was intercepted by a fraudster and the online access was set up.

Shortly after this James Hay received instructions through the online portal to update Mr S's email address and his mobile phone number. No additional checks were made to verify the instructions were from Mr S. His May 2019 monthly income payment had been made as usual, but from June payments totalling over £39,546 (net of tax) were requested to be paid to bank "B", along with instructions to sell units to fund the transfers. In September a payment of around 311,700 (net) was made to bank "H" and high value payments totalling over £82,000 to bank "I" for October, November and December 2019. So seven payments were made from Mr S's SIPP without his knowledge and without James Hay making any additional checks.

Mr S was on holiday in August 2019 and was away again in October 2019 retuning in January 2020. On his return he realised he hadn't been receiving his mail and no monthly income payments had been received to his account with S since May 2019. Mr S complained to James Hay and the fraud was discovered. Mr S feared his mail was being intercepted, as the mail boxes in his block of flats weren't entirely secure. Mr S is in his 80s and the situation has caused him significant worry and distress.

James Hay undertook an investigation, which discovered more than £133,500 had been withdrawn from Mr S's SIPP (compared to the £13,080 he was expecting for that period), reducing the balance from around £290,000 to £95,000. James Hay accepted that from September 2019, concerns should have been raised about the frequent, high value and out of character payments being made to multiple bank accounts. But they refused to repay the full amount as they had followed their security process for setting up the online access by sending a letter to Mr S's home address with the access code. They hadn't been made aware of concerns about the security of Mr S's mail and had no reason to suspect it wasn't Mr S himself setting up the access. So they offered Mr S an "ex gratia" payment of £93,991.03 being the total of four payments made between September and December 2019 (net of tax). And in January 2020 they credited £87,867 to the SIPP, being the tax reclaimed from HMRC.

Mr S rejected the offer as it didn't fully reimburse his loss. So he brought his complaint to this service. One of our investigators upheld the complaint and said James Hay should refund Mr S in full. He felt although James Hay had followed its own procedures, in this case they hadn't done enough to verify the instructions were coming from Mr S.

James Hay disagreed saying the investigator was applying hindsight, the security control of sending a letter to Mr S's home address was sufficient, plus they provided copies of letters sent to Mr S and his IFA, which they couldn't know hadn't been received.

As agreement couldn't be reached the case has been passed to ne to make 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.

It's not the role of this service to investigate the fraud itself or identify who's responsible, that's for the police. It seems the perpetrator was aware Mr S held substantial funds with James Hay and was able to intercept his mail to set up the online access and prevent Mr S himself being alerted to the fraud. This decision will simply consider whether James Hay did enough to protect Mr S's funds, and like the investigator I don't think they did.

I accept the first time a consumer requests online access to their account is by its nature "out of character" but not necessarily suspicious. And increasingly businesses may encourage their customers towards self-service channels. As the investigator explained we're not the industry regular so we don't generally comment on the way a firm conducts its business, as these are decisions they are entitled to make based on the risk they believe the situation presents. But James Hay must comply with the relevant regulatory and data protection requirements to protect the security of their customers' funds and personal information. So I've looked at what James Hay did to ensure it was acting on genuine instructions.

Mr S's personal and contact details

James Hay couldn't know Mr S's mail was at risk of being intercepted, indeed Mr S seems not to have suspected anything was wrong until January 2020. But James Hay's records include Mr S's date of birth, so it knew he's an elderly gentleman. James Hay has a copy of Mr S's lasting power of attorney (LPA) in favour of his two sons which his IFA encouraged him to establish due to his age. And in January 2019 James Hay received Mr S's "*expression of wish*" form which was completed in Mr S's hand and contained his email address (which is made up of his first and surnames) and mobile phone number, which were held on their system. They were also aware Mr S's usual contact method was telephone or handwritten letter. Mr S uses notepaper pre-printed with his address including his mobile telephone number and his email address which match those on the expression of wish form.

On 7 June 2019 James Hay received an online registration application purporting to be from Mr S. A user name was generated which was made up of Mr S's name and the two digits of his year of birth. The application quoted an email address not in Mr S's name including the digits "44" which doesn't reflect Mr S's year of birth or his address. As manual verification was needed, a letter containing an authorisation code would be sent to Mr S's home address. James Hay quickly received a message querying whether the access code would be sent out automatically or whether he needed to request it. This message quoted the same email address but also included a mobile phone number which was different from the one held for Mr S. A week later James Hay received a message through the portal headed "*change of personal details*" quoting the same email and mobile number asking how to

change the mobile number James Hay held as it was "*an old one I no longer use*". James Hay didn't think this was incongruous and replied on 20 June that personal details can be changed through the portal, by secure message or by sending a signed letter. And on receipt of the instruction confirmed the number had been updated on 8 July 2019. Once the online access was set up the other changes could be made with no further checks.

Mr S's bank account details

Mr S had received regular monthly income payments into his account with "S" for many years and ad hoc payments would be out of character. In June 2019 James Hay received two instructions for ad hoc payments – £4,800 on 17 June 2019 and £7,300 on 26 June 2019 to be paid to "Mr S's" account with bank "B". Units were sold to fund these payments.

On 20 August 2019 someone calling themselves "*Alan*" (not Mr S's name) called from the new mobile number asking how to change the bank details. The caller was told to send a secure message. Although no personal data was disclosed James Hay didn't seem alert to the discrepancy in the name or that the call might be suspicious. A secure message followed the same day saying Mr S had closed the bank account James Hay "*had on file*" (without giving those details) and providing the account details for the account with bank "B". Unfortunately this all took place before banks were required to verify that the number matched the account name which would have revealed the account did not belong to Mr S. James Hay received a secure message on 30 September 2019 apparently from Mr S saying he'd been called by his bank to say the September income payment of around £11,782 had been returned and wondered what would happen to the funds. He was told James Hay couldn't provide further information until the funds were returned but they'd be credited to his SIPP cash account. The caller doesn't appear to have been identified during that call.

Why I think James Hay did something wrong

James Hay admits concerns should've been raised from the 25 September payment to bank "H" followed by the three payments to bank "I". Although in fact they weren't suspicious even then, as the fraud was only discovered when Mr S queried his missing payments. In relation to the set-up of online access swiftly followed by the change of email address and mobile number and the new bank account with B James Hay says they had "*no reason …. to suspect the request had come from anywhere other than [Mr S] himself*". But I disagree. I think taken together the speed and out of character nature of the changes should have raised concerns from the outset, particularly given Mr S's age and potential vulnerability. Although James Hay was satisfied the instructions were genuine as they originated through the secure online access, as that had been set up fraudulently then any transactions made that way were also fraudulent.

A customer isn't obliged to explain their actions, but it's surely unusual for an elderly customer to change their email address, get a new mobile phone and change their bank details in about two months, so soon after setting up online access for the first time, and when they'd recently included those contact details on an important document like an LPA. So when James Hay received the first email which originated from a different email address than the one it held and which didn't even attempt to replicate Mr S's name, I think this should have raised concerns. Instead of sending a standard letter containing the code without having established it originated from Mr S, I consider it would've been reasonable to require an additional step to obtain the authorisation code. For example requesting a phone call whereby the caller would be taken through security. Of course this might not be fool proof as it's possible the fraudster knew enough of Mr S's personal data to answer the security questions. But having to impersonate Mr S might have acted as a deterrent. And it would have provided James Hay with the opportunity to ask further questions and assess whether the caller appeared to align with other details they held about Mr S (such as his age

and nationality), particularly relevant for an out of character contact from a vulnerable consumer.

James Hay's standard letter to Mr S's home address providing the authorisation code, explained that before online access to client data can be granted a number of security checks must be completed of which the security code is described as the "*last step in our security process"*. Understandably details of a firm's security procedures will be confidential. But given the contact did not originate from Mr S, wasn't in his usual format or from the email address James Hay held for him I'm not sure what other security checks they'd carried out. James Hay has confirmed its envelopes include information which would enable its correspondence to be identified. So the fraudster had been told to expect a letter containing the code it needed to activate online access and could do so without completing any identification checks and with no direct contact with anyone from James Hay.

James Hay is correct that they aren't expected to monitor how a customer chooses to spend their own money in retirement. But I can't fairly say it's just with hindsight the pattern of behaviour should have raised concerns. Mr S's income had been paid to bank "S" for many years and then in a short period of time he apparently changed his email address, mobile telephone number, and bank details and then made multiple payments of a higher value than usual, with no apparent rationale and without consulting his IFA. As each of the communications or changes involved a different person at James Hay nobody saw the full picture or considered whether things didn't feel right. It seems the possibility the account was vulnerable to fraud simply didn't occur to them.

I can see James Hay did send a number of confirmation notes to Mr S and his IFA confirming the actions it had taken (such as the new bank details or selling units) and to inform him that the payments he had made would be subject to tax due to the annual allowance being triggered. But that was standard procedure, the letters weren't sent because James Hay was suspicious and wanted to confirm the transactions were genuine. In any case it appears the fraudster was able to intercept the letters addressed to Mr S, who wasn't expecting them so didn't realise they'd gone missing. And the IFA's role was simply to advise Mr S on investment strategy a couple of times a year not to monitor how he chose to spend his pension fund. So his intervention might have presented an earlier opportunity for the fraud to be discovered rather than prevented it from happening. And I'm satisfied Mr S didn't make the changes himself or authorise anyone to make them on his behalf. Nor have I seen anything to suggest he acted negligently by sharing his personal information with a third party.

So while James Hay might be generally satisfied with its security protocol of sending a letter including the authorisation code to a customer's home address, in the circumstances of this case I don't think they did enough to protect Mr S's funds or to ensure they were communicating with him.

So I'm going to uphold the complaint and require James Hay Administration Company Ltd trading as James Hay Partnership to reimburse Mr S in full for his losses which was the solution proposed by the investigator. But I didn't think that went far enough to recognise the impact of the loss of the use of those funds for a sustained period of time.

In view of the length of time the matter had been outstanding and in recognition of Mr S's age and the distress the situation had caused him, I let James Hay know what I was proposing, and my understanding is they were agreeable to the proposed redress.

So this decision simply formalises that redress.

Putting things right

James Hay has set out the fraudulent payments as follows:

Date	Amount (net of tax)
25 June 2019	£5,712.97
29 July 2019	£6,848.17
23 August 2019	£26,985.02
25 September 2019	£11,782.87
28 October 2019	£33,782.87
26 November 2019	£45,442.42
23 December 2019	£2,982.87
Total	**£133,537.19**

James Hay should refund the total of these payments to Mr S. I understand it has already repaid £87,867 of tax reclaimed from HMRC.

In addition, for each payment James Hay should apply interest at 8% simple per year from the date of payment to the date of settlement.

And in respect of the worry and distress this has caused to Mr S James Hay should pay him £500.

My final decision

I uphold this complaint. James Hay Administration Company Ltd trading as James Hay Partnership should put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 24 December 2021.

Sarah Milne
Ombudsman