

The complaint

Mr F is unhappy that PrePay Technologies Limited trading as Prepay Solutions will not refund the money he lost after falling victim to a scam.

PrePay Technologies Limited trading as Prepay Solutions is responsible for answering complaints about payment services provided by Monese Ltd.

As Mr F's account is Monese branded, I have referred to Monese when explaining what has happened in this complaint as this is what he is most familiar with.

What happened

On 15 June 2020, Mr F fell victim to an impersonation scam. Fraudsters convinced him he was dealing with HMRC and had an outstanding tax liability. They told him he'd not responded to letters that had been sent to his address and threatened him with imprisonment if he didn't now comply. Mr F says he asked the fraudsters for proof and they told him to check the phone number they were calling from against the gov.uk website. Mr F recalls that the phone number matched with a number listed on the official government website. In the belief that this was his last chance to try and sort the situation out, he made 21 faster payments totalling £20,281 to four new payees between 14:28 and 18:11 that afternoon. He transferred money from his current account into his Monese mobile money account to make the payments.

Mr F explains he was convinced he was dealing with the genuine organisation because the fraudsters were very professional. He recalls that what he was being told about court and prison worried him. He's explained that he is a law-abiding person and that he wanted to make this situation go away as a criminal record would cause him problems with his work. He explains that the fraudsters managed to catch him at a particularly difficult time when he was stressed at work and not really thinking straight. Mr F has provided a copy of his work diary showing the high volume of meetings and commitments that he was juggling.

Despite feeling overwhelmed, Mr F can remember some details from the call. He says that the fraudsters told him that his bank would be too slow sending payments and asked him if he had another account he could use to pay. He told the fraudsters he held an account with Monese and they said to use that one instead. The fraudsters then told Mr F that the payments had not gone through, so he needed to make them again. Mr F says he was told that any overpayments he had made would be refundable when the matter was sorted out. He recalls feeling a range of emotions during a phone call that lasted well over three hours. He was angry that he'd never received the letters referred to and afraid of the authority of HMRC and the threats made.

Mr F has explained that he is not a British citizen, English isn't his first language and he wasn't fully familiar with HMRC and how it worked. He feels these factors made him more susceptible to what the fraudster was saying.

Mr F says he only realised he'd been scammed when it dawned on him that he's never been self-employed and that his employer pays his tax directly to HMRC. He reported the matter to the Police and Action Fraud, then contacted Monese the next day. In this call, Mr F explains that the fraudsters were "*very clever*" and that he "*lost control*" of the situation.

On 16 and 17 June 2020, Monese contacted the beneficiary institutions to try and recover the money he'd sent. Monese has not signed up to UK Finance's Best Practice Standards for the recovery of funds. Unfortunately, only a few pence remained.

Mr F was unhappy that Monese didn't stop or flag the transactions. He pointed out he never made transactions of this size so Monese should have noticed what was happening.

Monese did not uphold Mr F's complaint. In its final response, it explained that it had tried to recall the funds. It felt it had followed Mr F's instructions to make the payments in line with the terms and conditions of his account.

Unhappy with Monese's position, Mr F asked us to consider his complaint. Our Investigator looked into things and thought the complaint should be upheld.

He thought the transactions Mr F made were concerning and ought reasonably to have caused Monese some concern too. He thought Monese had missed an opportunity to ask further questions and identify what was happening. He thought there was an emerging pattern which could have been signs of financial harm evident from the fifth payment onwards, as by that point Mr F had moved money in and then swiftly out in order to make payments to three new payees within 40 minutes.

He thought if Monese had initiated a meaningful interaction with Mr F at this point, it would have made all the difference and stopped him from incurring further loss. He noted that Mr F had not been given a cover story to tell the business, so it's likely he'd have spoken openly and honestly about the situation he was in. He thought Monese ought reasonably to have recognised that Mr F's actions, by setting up new payees and rapidly emptying the balance of his account, bore the hallmarks of common scam activity.

In all the circumstances, he thought Mr F had acted reasonably and that he'd fallen victim to a sophisticated scam. He didn't think Mr F had acted negligently and contributed to his loss. He noted that phone number spoofing is a very powerful tool used by fraudsters. He also recognised that Mr F had less knowledge and awareness of HMRC and how tax affairs in this country work. He concluded that Monese should have done more and recommended that it refund all of the money lost starting with the fifth transaction Mr F made plus 8% simple interest. He also suggested that Monese should pay £250 compensation to Mr F to recognise the distress and inconvenience its actions have had on him. He noted the deterioration in Mr F's mental health after the scam.

Monese disagreed. It pointed out Mr F's current account provider didn't flag anything when he moved the money to his Monese account. It also raised that one-time passcodes were sent to Mr F for each new payee and he should have been aware that these beneficiary details did not have any link to HMRC. It said it could not have interacted with Mr F at the time because he was already on the phone to the fraudsters. It added the amount Mr F needed to pay increased and it was unclear why he believed that to be genuine.

It then said our Investigator's outcome was underpinned by a judgement in a court case, Quincecare. It felt a more recent court case had challenged that precedent and narrowed the duty of care owed to a customer.

Our Investigator told Monese he was aware of the recent Philipps v Barclays judgement where the judge took a different view about the Quincecare duty. He clarified he was not suggesting the Quincecare duty applied to this case. He pointed out that, notwithstanding what the judge recently said, we have a duty to resolve complaints based on what we think is fair and reasonable in all the circumstances of the case, taking into account not just the law, but also regulators' rules and guidance, relevant codes of practice and what we consider to have been good industry practice at the time.

Monese said it still did not agree and requested for an Ombudsman to review the matter afresh.

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.

The relevant law and regulations – plus good industry practice and Monese's own submissions – suggest Monese has a duty of care to protect its customers against the risk of fraud and scams so far as reasonably possible. Monese might be negligent and liable for reasonably foreseeable losses if, in breach of that duty of care, it fails to act on information which ought reasonably to alert a prudent authorised electronic money institution to potential fraud or financial crime by, or against, its customer.

Having said that, the Payment Services Regulations 2017 also indicate that Monese should execute authorised payment instructions without undue delay – and there is a presumption that liability for an authorised payment rests with the payer, even if that authorisation was obtained by third-party fraud.

There's no dispute in this case that Mr F authorised all of the disputed transactions. And I've taken the above obligations into account when deciding if Monese acted fairly and reasonably when it processed his instructions.

I am aware that Monese is not a bank. Nonetheless, in June 2020 when Mr F made these payments to fraudsters, transaction monitoring was firmly established as good industry practice and applied to electronic money institutions. I understand from Monese's submissions that it considers its duty of care to Mr F to be narrow. It has confirmed that Monese has systems in place to flag suspicious transactions, but these particular payments did not flag.

I have looked at what I think is at the heart of the matter here, being: should Monese have recognised Mr F's payments as being suspicious and intervened, and if it had done so, would it have made a difference to what happened.

We agree that the law recognises that a bank may be liable to its customer if it makes a payment in circumstances where it has reasonable grounds (although not necessarily proof) for believing that the payment instruction was an attempt to misappropriate the funds of its customer (this is known as 'the Quincecare duty'). I am mindful that the courts have interpreted Quincecare narrowly, but also, the circumstances of this complaint are different to that case. I'm not suggesting the Quincecare duty applies to this case. The judges in the Philipp and Quincecare cases Monese referred to were restricted to deciding the issues before them as pleaded by the parties in an adversarial process with strict evidential rules. It is unclear from those judgments whether they were invited to consider, in detail or at all, the overall regulatory landscape or general principles of good industry practice. Our wider investigatory remit permits us to take account of such matters.

I have a duty to resolve complaints based on what is fair and reasonable in all the circumstances of the case, taking into account not just the law, but also regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time. In this case, I need to decide whether Monese acted fairly and reasonably in its dealings with Mr F or whether it should have done more than it did. Mr F doesn't dispute he made each payment himself. So Monese had an obligation to follow his instructions and make the payments he requested. But there are some situations in which Monese should reasonably have a closer look at the circumstances surrounding a payment. As I've explained, I consider that as a matter of good practice Monese should've been on the lookout for unusual and out of character transactions.

The activity on Mr F's account that day does stand out as being unusual for him. I understand Mr F has held a Monese mobile money account since March 2020. I've looked carefully at his account statements and I can see that the transactions he made on the day of the scam were very different in character to the type of transaction he typically made. His spending was usually low value contactless transactions in supermarkets and for public transport. His account balance was typically modest and tended to be no more than £100. But during the period of the scam, there's a significant increase in account movements, for much higher values than Mr F has ever spent, and to four new payees. I consider these factors to be signs that could indicate financial harm.

Mr F made 21 payments in around three hours. The rapid emptying and replenishing of the account to utilise over £20,000 in around a three-hour period is significantly out of character for him and I think out of character for how an account held at an electronic money institution would typically be expected to run. Monese's product information explains that a cardholder is allowed to make 50 transfers each month, meaning Mr F had utilised a significant proportion of those within hours. Monese did not challenge any of these payments at the time of the scam.

Having looked at the transactions, initially I don't think Monese would have had sufficient reason to be concerned that Mr F might have been at risk from financial harm from fraud. To begin with, the money Mr F transferred in and then out to a new payee was unremarkable in and of itself. But by the fifth payment Mr F made, I consider it was clear that something unusual was happening on Mr F's account.

At this point, a troubling pattern of spending has developed. I think Monese should have fairly and reasonably recognised that the activity unfolding on Mr F's account was concerning. Mr F had made five payments to three new payees in approximately 40 minutes. He'd moved money into his account four times to make these payments and then rapidly utilised it all. I think that Monese should have done more to satisfy itself that there was no potential fraud or financial crime by, or against, its customer.

Having established that Monese ought to have intervened, I am also persuaded that its intervention at this point would have made a significant difference and ultimately prevented Mr F from sending any more money. When making that decision, I have based my findings on the balance of probability – that is, what I think is more likely to have happened, taking into account what I know from the information that is available to me.

If Monese had correctly identified this pattern of spending as being unusual, I'd have expected it to have contacted Mr F to ask questions about the nature and purpose of the payments he wanted to make.

Monese raised that it could not have interacted with Mr F during the scam as he was already on the phone. It's unclear whether Monese only had a mobile number for Mr F or not. I am also mindful that app-based organisations can have different arrangements for account servicing and may not have dedicated call centre staff readily available. But I've not seen anything that makes me think Monese could not have blocked payments which would have resulted in Mr F needing to interact through the usual servicing channels in order to proceed.

By not blocking the account, an opportunity to force Mr F to interact was missed. I think forced interaction would have prevented further payments from being made. It would have given Mr F reflection time and most likely taken him out of the environment created by the fraudsters. If Monese had been in contact with Mr F, it is more likely than not that it would have had concerns about what was happening even if Mr F did not. I am persuaded that sharing those concerns would have stopped Mr F from sending any more money.

I've thought carefully about the points Monese has made in response to our Investigator's position and I still think that Monese should have done more than it did and that doing so would more likely than not have uncovered what was happening and prevented Mr F from incurring any further loss.

Monese suggested that Mr F's bank could be responsible for the loss as they didn't flag anything unusual either. But in this case, Mr F transferred money from his bank account to another of his accounts held with Monese and from that account to the fraudster. I'm satisfied it wasn't the transfer of funds from Mr F's current account (or his bank's failure to intervene in those transfers) that caused the loss. Mr F wouldn't have suffered a loss at all had it not been for the transfer from his account at Monese to the fraudster and that, I think, is the actual cause of his loss. I can't fairly hold his bank responsible for Mr F's loss as the loss hasn't been caused by its actions.

Monese pointed out that it had sent Mr F one-time passcodes each time he set up a new payee and he should have been aware that these beneficiary details did not have any link to HMRC. Whilst I recognise that Monese feels Mr F ought to have realised that a genuine organisation wouldn't require Mr F to pay individual accounts held at different institutions, I think Monese has placed insufficient weight on the environment created by the fraudster. In impersonation scams, fraudsters are masterful at providing cover stories that are plausible and are often coaching their victim to explain away concerns. The environment created by the fraudster is one of fear and panic, making it more difficult for a consumer to think rationally. We know fraudsters are very good at manipulating people and persuading them to do things they would not do in the cold light of day, away from a highly pressured environment. This is evident from Mr F's reflection on the situation where he has explained that he does not know what "*switched in his mind*." But Mr F does not have the same level of knowledge that a financial business has about what well known scams like this look and feel like.

Monese has raised concerns about the plausibility of the situation Mr F was in. It points out the amount he needed to pay kept increasing and it was unclear why he believed that to be genuine. But Mr F has described how the scam caught him off guard and at a particularly busy time at work. He's explained that he was unable to think clearly. With hindsight, Mr F blames himself for realising it was a scam so late. From what Mr F has said and described, the environment created by the fraudster convinced him he was genuinely interacting with HMRC. It's clear from what he's said that the combination of stress, fear and panic disarmed him. The sophistication of the scam is relevant here. Mr F was afraid of the consequences of arrest and court action on his employment and immigration status. He felt the fraudster's processes and method of operation, including the spoofing of a number linked to a genuine UK government agency, made those threats real ones. I don't think it is fair and reasonable to expect Mr F to have realised he was being scammed sooner.

The checks and measures a business undertakes should be proportionate to the relationship that exists between it and its customer. The way Mr F was using his account when unwittingly transferring his life savings to fraudsters was unusual for him. It matched a pattern indicative of fraud and it was different to what Monese knew about the way Mr F's account usually ran.

Monese has said that it does have systems in place to look out for fraud. Against this backdrop, I'm not satisfied Monese did enough to try and protect Mr F from financial harm in the particular circumstances of this complaint.

Whilst I recognise that Monese is an electronic money institution, its mobile money account encourages usage akin to a current account, including bill payments, purchases and other everyday spending. Although Mr F was not a long-standing customer, he had been an active customer for around three months and had built up a pattern of day to day spending that can be identified as normal for him. At the very basic level, the activity on the account on the afternoon of the scam was a change to Mr F's usual usage, which I think Monese ought reasonably to have detected, in line with its duty of care and good industry practice.

Taking into account the firm's obligations, as well as the particular circumstances of this complaint, I do not think Monese acted fairly because it did not do enough to try to protect Mr F from financial harm from fraud. I consider that this has had a detrimental impact on Mr F. I'm persuaded Monese missed an opportunity to detect that something was amiss and that it more likely than not would have prevented Mr F from suffering any further loss if it had intervened appropriately. In the circumstances, I am satisfied that it would be fair and reasonable for Monese to refund the money lost from the fifth payment onwards.

I also think it is appropriate to make an award of £250 for the distress and inconvenience Mr F has suffered. He's understandably found things difficult since the scam. It's a lot of money for anyone to lose. Mr F tried to contact the fraudsters after the scam to ask for them to return his money as it was all of his savings and he'd worked hard to build them up. It's clear the fraudsters robbed him of more than just money, it was his future plans that now will take longer to realise. In reaching that conclusion, I'm aware that his loss was ultimately caused by the actions of the fraudsters but remain mindful that Monese could ultimately have prevented the extent of the harm that he's suffered.

My final decision

For the reasons I've given, my final decision is to uphold this complaint and require PrePay Technologies Limited trading as Prepay Solutions to:

- Pay Mr F the money he lost from the fifth transaction onwards (£16,482).
- Pay 8% simple interest per year on that amount, from the date of the unauthorised transactions to the date of settlement (less any tax lawfully deductible).
- Pay Mr F £250 distress and inconvenience to recognise the impact its actions have had on him.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 30 March 2022.

Claire Marsh

Ombudsman