DRN-6270400

The complaint

Mrs T complains that Currensea Limited ("Currensea") is holding her liable for payments that were taken from her account as a result of a scam.

What happened

In summary, in May 2025, Mrs T received a call from someone claiming to be from the Police. This caller (who was in fact a scammer) told her she had been targeted by fraudsters and gave her a "crime reference number". On 29 May 2025, she received a second call from another scammer, this time pretending to be from her personal bank ("Bank N"). This scammer provided the "crime reference number" she had been given in the first call.

The second caller said Mrs T's email account had been hacked and monitored for several weeks. Mrs T says this corresponded to an email she had received earlier that day notifying that her account had been linked to an unfamiliar device. Believing the caller was genuine and helping to stop fraud, Mrs T was persuaded to share her email password. And worried about the safety of her money she shared her card and security details for various accounts, including those for her Currensea account. She says she was persuaded to delete texts from her banks, including those containing security codes, after sharing the information.

After some hours, the scammer said they would call again the next day. But on speaking to her daughter Mrs T realised she had been scammed. She contacted Currensea (and other banks) to report what had happened. By that time, several payments had been taken from her Currensea account. Although Currensea agreed not to hold Mrs T liable for transactions made after she had reported the scam, it held her liable for the earlier ones below.

	Date	Method	Merchant	Amount
1	29-May-25	ApplePay - card present	B	£50
2	29-May-25	ApplePay - card present	B	£30
3	29-May-25	Online - 3DS	F	£425.99
4	30-May-25	ApplePay - card present	E	£48
5	30-May-25	Online - 3DS	S	£205
6	30-May-25	Online - 3DS	S	£205
7	30-May-25	Online - 3DS	G	£239.97
8	30-May-25	Online - 3DS	G	£89
9	30-May-25	Online - 3DS	G	£89
10	30-May-25	Online - 3DS	S	£209
11	30-May-25	Online - 3DS	S	£175
12	30-May-25	Online - 3DS	G	£100

Mrs T complained to Currensea. She was unhappy it held her liable on the basis that she had been grossly negligent in failing to protect her account. She referred her complaint to our Service. Our Investigator upheld it. He concluded the payments were unauthorised. While Mrs T shared information that allowed the scammer to make the payments, she believed she was protecting her funds. He also found that while Currensea could hold Mrs T

liable for the in-person ApplePay transactions on grounds of gross negligence, there was no provision to hold her liable for the online transactions, as these were distance contracts.

He recommended a refund of payments 3 and 5-12. He said this should go to reducing the balance owed and that Mrs T should be given the standard term to repay what remains. He also said Currensea should remove interest and charges incurred on the refund amount, remove entries and adverse data, and pay £50 for the lack of service provided post-scam.

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.

Having done so, I've decided to uphold it for similar reasons as the Investigator.

Authorisation

The starting point – under the Payment Services Regulations 2017 (PSRs) – is that Mrs T is liable for payments she authorised. With some limited exceptions, Currensea is liable for unauthorised one. In this case, it's not in dispute Mrs T was the victim of a scam. It also doesn't seem in dispute she didn't make any of the payments herself. The scammer did, using her card details and credentials to set up ApplePay and the app on their devices.

As the Investigator noted, and as Currensea also explained, the evidence shows that the account was accessed from a new device, belonging to the scammer, at 22:31 on 29 May 2025. A verification process was completed within minutes on that device linking it to the funding account. Using Mrs T's card details, the scammer added her card to their ApplePay. They used that to carry out some 'card-present' transactions and also used the card to initiate several online payments (many of which were declined) to various merchants. These online transactions were approved in-app, but from the scammer's device.

Mrs T doesn't dispute providing the scammer with the information, including card details, password, and one-time passcodes (OTPs), that enabled them to make all the payments. However, she has consistently explained she did so believing she was speaking to Bank N's fraud team. She said they already knew sensitive information about her, such as name and email address, and that an earlier call from someone pretending to be the Police, along with an email about an attempt to link an unfamiliar device to her account, made the caller appear more credible. She has explained that, at a time of worry and panic, she was persuaded to follow instructions from who she thought was a trusted source protecting her money.

I find Mrs T's explanation plausible. She neither made the payments herself nor instructed Currensea to make them. And I'm not persuaded her actions, or her understanding of the situation, amounted to giving consent for another person to make payments on her behalf. I'm therefore satisfied the payments were unauthorised. It appears Currensea accepted this initially given that in its complaint response and file submissions, it said Mrs T was liable on the basis that she had been grossly negligent in failing to keep her security credentials safe.

Online payments – distance contracts

The PSRs set out the circumstances in which Currensea can hold Mrs T responsible for unauthorised transactions. However, under Reg 77(4)(d), a payment service provider can't hold the account holder responsible for an unauthorised payment if their payment instrument is used in connection with a distance contract, other than an "excepted contract".

Payments 3 and 5–12 were made online. I consider them to be distance contracts and there is no indication they more likely related to “excepted contracts”. While Currensea says these were not distance contracts because Mrs T was not a party to the contracts, the PSRs refer to the use of the “payment instrument” in connection with a distance contract. They don’t require the account holder to have entered the contract. As I’m satisfied the online payments were unauthorised and distance contracts, Currensea cannot hold Mrs T liable for them.

ApplePay payments – in person

Payments 1, 2 and 4 were made in person. Currensea can hold Mrs T liable for these unauthorised payments where Mrs T failed with intent or gross negligence to take all reasonable steps to keep safe her personalised security credentials.

In considering if Mrs T failed in her obligations, I’m considering if she seriously disregarded an obvious risk, falling significantly below the standards expected of a reasonable person in that situation. Our Investigator thought that the bar for gross negligence has been met. Mrs T hasn’t disputed this. And I’ll briefly explain why I agree with this position.

The scam began when Mrs T received a call from someone claiming to be from the Police, telling her she had been targeted by fraudsters. She received a second call from someone claiming to be from Bank N, who said her email had been compromised and was being monitored. Mrs T explained that the caller knew certain details about her and that their use of the earlier “crime reference number” made them seem credible. As before, I accept she believed she was speaking to a trusted source who was helping her protect her accounts.

At the same time, both calls came from ‘unknown’ numbers. When asked what information the callers knew about her and how she verified their identity, Mrs T’s response was that this was limited to her name, email address, and possibly her home address. She also explained she was instructed to ignore and delete notifications, including security codes, and “pushed” not to accept any calls. I can’t see she was given a plausible explanation for why this was necessary or how a fraudster would have obtained that information. Like the Investigator, I also consider most people in these circumstances would have questioned why someone from one bank required extensive security details, including usernames/passwords, for other providers or how such information would be used to secure accounts of unrelated firms.

Taking everything into account, I consider that Mrs T did ignore an obvious risk by failing to take reasonable steps to verify the caller’s identity and sharing the information she did, such that her actions fell significantly below the standard expected of a reasonable person in that situation. For these reasons, I’m persuaded that, in this case, Currensea can hold Mrs T liable for the unauthorised ApplePay payments.

Prevention

There are some circumstances where I would expect a firm to take extra steps or carry out additional checks before processing a payment, for example, when a transaction appears particularly unusual or suspicious.

I understand Mrs T’s point that her card was rarely used and only when she was abroad. However, having considered the account activity, including payment values and merchants involved, I don’t think there was enough for Currensea to have intervened on concerns that Mrs T was at a heightened risk of fraud at the time the ApplePay transactions came about.

As I’m not persuaded that Currensea missed an opportunity to prevent those losses, Mrs T remains liable for the ApplePay transactions for the reasons already explained. And because I’ve already found Mrs T is not liable for the online transactions, I don’t need to consider

what would have happened if Currensea had intervened on those payments.

Other matters

A possible recovery route for the ApplePay transactions was the chargeback scheme. However, I'm satisfied that any such claim was unlikely to succeed, as the merchants would most likely have provided the goods or services, albeit to a scammer.

The Investigator also said that Currensea should compensate Mrs T for the distress and inconvenience caused by how it handled her claim. Currensea hasn't disputed this. I can see no reason why it couldn't have taken the time to talk things through with Mrs T, as she had requested, at an already difficult time. I consider £50 to be fair in the circumstances

Putting things right

To put things right Currensea Limited needs to remove the unauthorised online payments from any balance, along with any associated interest and charges; remove any adverse entries relating to the unpaid balance; and pay Mrs T £50.

My final decision

For the reasons given, I uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs T to accept or reject my decision before 30 April 2026.

Thomas Cardia
Ombudsman