DRN-4693515

The complaint

Ms E complains Starling Bank Limited ("Starling") won't refund transactions she didn't authorise.

What happened

The details of this complaint are well known by both parties, so I won't repeat them again here in detail. Instead, I'll focus on setting out some of the key facts and on giving my reasons for my decision.

I'd like to assure Ms E that I have received and reviewed the documents that were physically brought to this service on 1 October 2024. It's important to note that this decision relates to Ms E's personal and sole trading account with Starling.

In March 2023, Ms E raised a claim with Starling that she didn't make several payments, made by card, to an online retailer for discounted goods and services on 10 February 2023. I'll refer to this retailer as "G" going ahead.

Ms E later made further claims that she hadn't authorised payments through a variety of payment methods including online card subscription, online banking, contactless, ATM and using Faster Payments dating from 2021 to May 2023. I will not list them out here given it would be impractical to do so.

Ms G says she's been the victim of fraud mainly through the following:

- her phone and Google account were hacked
- debit cards were intercepted
- third-party software has been used to take over her devices
- her identity has been stolen

As Starling didn't refund Ms E for the transactions she disputes to having made, she complained. Starling didn't uphold Ms E's complaint, in summary, it made the following key points:

- It hasn't found any evidence of fraud. The transactions were authorised from Ms E's device

- There's no evidence which shows Ms E's online banking was accessed via a compromised device

- The transactions on Ms E's account, including those moved to saving 'spaces', don't support Ms E's contention they were fraudulent

Ms E referred her complaint to this service. One of our Investigator's looked into it, and they recommended it wasn't upheld. Their key findings, in short, were:

- Had there been a point of compromise of Ms E's account security credentials, she would be expected to change this upon discovery. And if the information was compromised in October 2022, its unlikely a fraudster would wait so long before using it to their benefit

- There's no evidence to show Ms E's phone was taken over by third-party software. And intercepting a physical debit card would require access to mail – and the creation of a virtual card would need access to Ms E's phone and app. There's no evidence to support either here

- Ms E hasn't provided clear examples of discrepancies on her account balances shown on her phone against those on the statements. Statements are a definitive record of the accounts, and any disputed activity can be identified on them

- Ms E reported ten transactions she says she didn't authorise to G totalling around £285. Starling's records show these transactions were made on her phone and some were authorised using 3DS Biometrics. And this wouldn't have been possible had the phone been taken over. So it's not likely an unauthorised third-party made them

- Spending occurs on Ms E's personal account until it nears zero, after which it stops. But it starts again once benefits are credited. Because of this its likely Mr E was aware of her balance and of the transactions that had taken place. So she should have reported them sooner

- Ms E reported several transfers to a third party, Mr W, between 21 April 2023 and 29 April 2023 as unauthorised. Ms E made transfers to Mr W before and after those she disputes which haven't been disputed. They can't see why a fraudster would make payments to an existing payee that's been set-up as early as 2021.

  Starling attempted several times to gain more information about these payments, but Ms E didn't respond. So its reasonable for Starling to treat them as authorised

- Ms E reported unauthorised card transactions to various retailers in April 2023 and said her new card had been intercepted. But some of these had been done with the previous card and for undisputed transactions.

  The ATM withdrawals would've required the card and PIN. There's no evidence of how a third-party would've been in possession of this. And if an unauthorised third – party did have them, it's unlikely they would make small value withdrawals and leave a significant balance in the account

- Ms E says her 'spaces' savings balance disappeared. But they are not separate accounts, so they would show on a statement. Ms E had several 'spaces' set-up on her account and there's no evidence of balances going missing

- Ms E says she deposited £20,000 into her business account, and it disappeared. Despite several requests, Ms E hasn't provided any evidence of this. If she does have any related information, she should report this issue to Starling to look into

Ms E didn't agree with what our Investigator said. In response, Ms E emphasised she has been the victim of fraud, and £20,000 has gone missing from her business account. She also says her other banks accept she's been the victim of fraud and refunded her around £1,300.

As I've already said, Ms E has recently provided more information to this service. She should note that I have still referred to her as Ms E and not by the Deed Poll name she has sent in. That's because I can't be satisfied that this document has finalised the process of changing her name given its a declaration, undated, and isn't a formal declaration of acceptance by the relevant authority.

She's also sent paperwork from her external bank and Action Fraud. And most notably, paperwork about her mental health and acute condition related to this. I'd like to assure Ms E that I've thought about this with care when reaching my decision.

Relevant considerations

When considering what is fair and reasonable, I'm required to take into account: relevant law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time.

Of particular importance to my decision about what is fair and reasonable in the circumstances of this complaint, are the Payment Services Regulations 2017 (the PSR 2017) which apply to transactions like the ones Ms E disputes. Among other things the PSR 2017 include the following:

Regulation 67 of the PSR 2017 explains:

> 67.— (1) A payment transaction is to be regarded as having been authorised by the payer for the purposes of this Part only if the payer has given its consent to —
>
> (a) the execution of the payment transaction; or
> (b) the execution of a series of payment transactions of which that payment transaction forms part

Whether a payment transaction has been authorised or not is important because account holders will usually be liable for payments they've authorised and, generally speaking, payment service provider's will be liable for unauthorised payments.

As there's no agreement, this complaint has been passed to me to decide.

What I've decided – and why

I'm very aware that I've summarised the events in this complaint in far less detail than the parties and I've done so using my own words. No discourtesy is intended by me in taking this approach. Instead, I've focussed on what I think are the key issues here. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

If there's something I've not mentioned, it isn't because I've ignored it. I'm satisfied I don't need to comment on every individual argument to be able to reach what I think is the right outcome. I do stress however that I've considered everything Ms E and Starling have said before reaching my decision.

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 have decided not to uphold Ms E's complaint.

I'm satisfied from Starling's technical records that Ms E's disputed transactions were

authenticated in line with what the PSR's say about this. In other words, they were authenticated in line with Starling's security processes. But the PSR's say that is not, on its own, enough to enable Starling to hold Ms E liable.

I also need to think about whether the evidence suggests it's more likely than not that Ms E consented to the payments being made. Having given this careful thought. I'm persuaded, on balance, that its most likely Ms E did consent to the transactions she disputes. I know she feels strongly about this. I'll explain why.

Payments to G

These payments were all carried out on the same day in February 2023 of which there were ten amounting to around £285 in total. Ms E reported them some time later in March 2023. Starling's records show the payments were made from a registered device, from the same IP address and using the card credentials. With some of these payments, Starling carried out further security by using 3DS and biometrics. Essentially this meant someone would have to go into the banking app and authorise them as not fraudulent.

This was done. Ms E says that her account was hacked as someone had hacked her Google account to get the security credentials as these were mutually the same. But I haven't seen any evidence that Ms E's Google account was hacked in this way. I also question why an authorised person would then carry out small value payments to a discount voucher retailer, when they could've utilised all the funds in the account.

I also note Ms E has said that she was led to add a third-party piece of software that allows her phone to be take over remotely. If that was the case, they would still need to know Ms E's security credentials to use her mobile banking app. I'd also add that I haven't seen any compelling evidence this is what happened.

Transfers to Mr W

Ms E had been making transfers to this beneficiary from 2021, and after the point she reported the April 2023 payments as fraudulent. Ms E has also sent statements for this individual which suggests she has a trusted relationship with them.

Given the likely proximity of Ms E's relationship with Mr W, and as transfers continued to be made after the alleged fraud, I must question the credibility of this testimony. I say that because if Ms E didn't authorise these payments, she should've been able to recover them. And if not, why would she continue to make them. I also note that the payments to Mr W were all made form the same registered device and IP address, and a device Ms E has said on a call I've listened to belonged to her.

Card transactions and ATM withdrawals

Ms E says that someone has intercepted her debit cards and carried out transactions on them which she didn't authorise. But some transactions were carried out on a previous card which had been used for other undisputed transactions – and either side of those reported.

Ms E hasn't been able to explain how someone would've known her PIN to carry out these transactions. It also appears she still has possession of these cards – so someone would have had to take them and put them back without her knowing. This seems unlikely – especially as funds weren't depleted from her account for maximum financial gain.

There's also no evidence of Ms E's card being intercepted or there being an issue with her mail. I also note that the disputed transactions would've had to have been carried out on two

separate cards, which also makes the likeliness of fraud being carried out less likely.

Account discrepancies

Ms E says that funds have gone missing from her account and there's discrepancies on what shows on her statements and that on her banking app. This could be explained by the saving 'spaces' she has set-up on her account. I say that because they would naturally show different balances to the overall statement. I also haven't seen any compelling evidence from either party that any funds have disappeared in the way Ms E says.

£20,000 deposited on business account

Ms E has said that she deposited £20,000 into her business account around the time it was opened. Both Ms E and Starling have provided statements which don't show such a deposit. This amount is also significantly out of character given the normal account balance and activity.

Given the significant value, I do question why Ms E hasn't raised this issue from the offset with Starling. And she hasn't provided any evidence of depositing this money like where it came from, a deposit slip, and how it was made. Despite several requests for such information, Ms E has failed to send anything to us.

If she later does recover any information that shows she deposited these funds, she should raise this with Starling to investigate.

Other points

Ms E says her external bank has accepted she's been the victim of such a complex, multi-faceted and sophisticated fraud. To support this she has sent in letters from this bank. One shows that she has been given a temporary refund in March 2024 of £470. And another shows a temporary refund was given of £60. Both letters don't show that Ms E was victim of the type of fraud she has described to this service. What another bank does isn't evidence that a claim against another bank should be upheld. After all each transaction needs to be investigated by the relevant bank in line with its obligations.

Ms E has also shown that she has reported fraud to Action Fraud. But this doesn't show what the outcome of any resulting investigation was. So I don't think its evidence I can put much weight on here.

Lastly, Ms E has sent me excerpts that review the online security strength of various financial providers. I note also they talk about similar types of fraud existing to that which Ms E has described as affecting her. I have taken this onboard, but for the reasons above, I'm persuaded on balance, that its most likely Ms E or someone else she's given permission to, has authorised the transactions disputed here.

My final decision

For the reasons above, I have decided not to uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms E to accept or reject my decision before 8 November 2024.

Ketan Nagla
Ombudsman