DRN-4473269

The complaint

Mr M has complained about NewDay Ltd (trading as Aqua) holding him liable for a credit card which he says he didn't take out.

What happened

Both sides are most familiar with the case, so I'll summarise what happened in brief.

In January 2019, an Aqua credit card was taken out in Mr M's name. It was used over several years, including for a money transfer to Mr M's personal account. It received regular repayments from a business account in Mr M's name.

In 2022, Mr M said he didn't take out or use this credit card. He said it had been opened and used by his former employer, who he'd given copies of his ID to, and his ex-employer had taken control of his bank account.

NewDay held Mr M liable for the debt. The card and PIN had been sent to Mr M's genuine address along with regular statements. And Mr M's bank said there'd been no third-party access to the account and Mr M had continued to use online banking on his genuine device.

Our investigator looked into things independently and didn't uphold the complaint. Mr M appealed, so the complaint's been passed to me to decide.

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.

Though I've carefully considered everything both sides have said, I will focus my decision on what I've found to be the key points.

I've found that NewDay are entitled to hold Mr M liable for this account. I'll explain why.

The credit card was applied for using Mr M's correct key details. NewDay carried out checks, which did not find any indication that the account was being applied for by anyone else.

While the email and phone number Mr M gave us do not match those used on the application, this is not conclusive either way. It's technically possible they were someone else's contact details. But it's equally possible that Mr M can have more than one phone number or email address, or that he changed his contact details over the years.

A large money transfer was made from the credit card to Mr M's personal account. Mr M says that he stopped using that account in late 2019, and that his ex-employer took control of it. But I can see that Mr M continued to access his mobile banking from the same mobile device he was using for his genuine activity before, which had been registered with the phone number he confirmed as being genuine, from IP addresses which matched up to IP addresses he used before. He continued to received income into that account, and it continued to be used for day-to-day spending consistent with Mr M's previous spending, at many of the exact same locations he usually went to before. He continued to receive statements, but didn't tell his bank anything was wrong at the time. And his bank confirmed there'd been no third party access to Mr M's account. So I'm reasonably satisfied that Mr M was using that account, meaning he received and benefitted from the money transfer.

Similarly, repayments were made from a business account Mr M was registered to. Again, this account was accessed from Mr M's device at IP addresses he'd used before.

It is not likely or plausible that a fraudster would make repayments towards their fraudulent spending for years, continue to pay their victim a wage for a long time after they'd stopped working for them, or transfer large sums of money to their victim. But that activity is very consistent with the possibility that this was Mr M's credit card.

The card and PIN were sent separately to Mr M at his genuine address, as were monthly statements which were addressed to him by name. It is not likely or plausible that his ex-employer would be able to access his post and intercept both the card and PIN, nor that they could then intercept all his statements for years on end. And Mr M confirmed he received other letters – indeed, he said he discovered this account and other accounts by receiving letters. Mr M says a fraudulent mail redirect was put in place in 2022, but that's not relevant to the card and PIN being sent to him in 2019, nor to the statements he was sent between 2019 and 2021. I don't see a likely or plausible way that someone could've got the card, PIN and statements without Mr M's consent and without him ever noticing something was wrong. I think it's most likely that Mr M was aware of the credit card and it's activity at the time, from the statements he received. Yet he didn't tell NewDay anything was wrong until 2022. And he would not wait so long if the account had been opened or used without his consent.

While I appreciate that other businesses may have chosen not to hold Mr M liable for other debts, we look at each case on its own merits. And in *this* case, there is substantial evidence which strongly suggests that this was Mr M's account. Whereas I've found no evidence which reasonably shows or substantiates that anyone other than Mr M applied for this account. Indeed, there doesn't seem to be a likely or plausible way that all the activity could've taken place over so long without Mr M's knowledge or consent.

On that basis, I find it was fair for NewDay to hold Mr M liable for the account. This is a difficult message for me to give, and I know it's a difficult message for Mr M to receive. But given the evidence and circumstances at hand, and the balance of probabilities, I'm unable to reasonably reach any other conclusion.

My final decision

For the reasons I've explained, I don't uphold Mr M's complaint.

This final decision marks the end of our service's consideration of the case.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 28 December 2023.

Adam Charles
Ombudsman