DRN-4882271

## The complaint

Mr S has complained that American Express Services Europe Limited (AESEL) (Amex) won't refund him for transactions' he says he didn't make or authorise totalling just over £60,000.

## What happened

The detailed background of this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Mr S has an Amex credit card account. Three other members of Mr S's family have supplementary cards for the account.

Mr S says transactions carried out on his Amex card totalling just over £60,000 were not carried out by him. As the account holder AESEL, holds Mr S liable.

Mr S says his Amex card was stolen, his email was hacked, and fraudsters opened accounts in his name, and used his card to purchase goods. So, Mr S says he shouldn't be held liable for the for the transactions.

Mr S says his wallet containing his AESEL card and other bank card was stolen sometime between 25 and 29 Aril 2023. Mr S says all of his bank cards including his AESEL card have the same PIN. Mr S has explained that he wasn't in London when some of the transactions took place and was out celebrating his birthday with his family. And that he has never visited the places where his card was used. Mr S says he only discovered the transactions then he found out that the supplementary card holders cards stopped working, which led him to check his account. Mr S said that he had not disclosed his banking PIN or banking credentials to anyone. And that no one had access to his mobile phone.

The disputed transactions took place between 30 April 2023 and 5 May 2023. They are well known to both parties, so I don't need to detail them here. It's noteworthy however, that most of the transactions are for high end goods, bought at luxury retailers.

Two transactions were especially high value - £26,599.99 for gold bullion bought at a retailer I will refer to as C on 2 May 2023, and a keyed transaction for £24,500 on 5 May 2023 to a business I will refer to as A. The keyed transaction as authenticated with a push notification via online banking.

Amex decided not to refund the disputed transactions. It felt that the available evidence suggested Mr S had authorised the transactions out of his account. In summary they said:

- Mr S's genuine card and PIN were used to carry out the transactions.
- The chip mechanism on the card has been read and validated for each transaction. As the chip mechanism on a card cannot be duplicated the genuine card has been presented for each charge.
- No new PIN was requested or viewed prior to any of the disputed transactions.

- Mr S confirmed via email that the transactions were not fraudulent.
- Mr S hadn't provided any evidence that his emails had been hacked.
- The fraudulent transaction on 2 May 2023, for £26,599.99 included £67.20 for membership renewal in Mr S's name. The membership was renewed for Mr S's genuine business, who confirmed business details were given including Mr S's email address with purchases.
- On 3 May 2023 AESEL again sent a fraud protection alert to validate charges to two retailers for £1,678.00 and £85.00. AESEL received a response the same day via email confirming the transactions as genuine.
- On the 18 May 2023 Mr S told AESEL fraud protection department that his email was hacked. No evidence was provided to support this claim.
- The payment to A was verified via a push notification being sent to Mr S's online account which was accessed using Mr S's trusted mobile device.

Mr S wasn't happy with AESEL's response. So, he brought his complaint to our service. He maintained he never made the transactions. So, he wants Amex to refund him the transactions because he is a victim of fraud.

One of our investigator's looked into Mr S's complaint. She asked Mr S some more questions about what had Mr S maintained that he never made the transactions and that someone must have hacked his account after stealing his wallet containing his Amex card. On balance, our investigator found that Mr S authorised the transactions. So, Mr S, as the account holder, is liable for them. In summary they said:

- There wasn't an explanation to show how an unauthorised individual would have known Mr S's Amex PIN.
- It's unclear why a fraudster wouldn't make use of all of the bank cards that were in Mr S's wallet after he says it was stolen.
- AESEL sent a number of alert messages to Mr S's registered mobile device and email address to confirm the disputed transactions and received responses that the transactions were genuine.
- AESEL confirmed the payment of £24,500 to A was approved in Mr S's banking app via MYCA using M S's mobile phone. In order for this to happen an unknown third party would need to know Mr S's banking app login credentials and password. And there was no plausible explanation how this could happen.
- There's no plausible explanation for how unknown third party would have known M S had an old account with C, and then gone to C and reopened the account using Mr S's correct contact details – including the name of Mr S's business, telephone number and email address.
- AESEL were fair to close Mr S's account.

Mr S disagreed with what the investigator said. He said he didn't carry out the transactions. So, he says Amex should refund the transactions. And shouldn't have closed his account. In summary he said:

- Fraudsters went to C and reopened an old account he hadn't used since 2021. He said fraudsters must have checked Companies house to find his company and address details.
- It's likely that an employee at C was complicit in the fraudulent transactions.
- Mr S was elsewhere when the transactions took place at C. He has visited C and discovered that fraudsters simply reopened his old account without having to provide any ID. And then proceeded to buy gold bullion.
- All of his other credit cards have the same PINs, not his debit cards. He hardly uses his debit card for anything, only transactions online.

- To get his Amex PIN the fraudsters most likely called Amex or got it by accessing online accounts or saw him using his card.
- He didn't receive any text messages to alert him to the fraudulent activity and his email access was changed.
- Fraudsters spoke to Amex. The theft team from Amex called Mr S and confirmed he was being impersonated during a phone call about his account.
- Mr S never approved the transaction to A. Fraudsters logged in and changed his passwords to his accounts. And hacked his email which is linked to his Amex account to carry out the transaction.
- He hasn't given his mobile phone to anyone else.
- Amex never carried out a proper fraud investigation and obtained CCTV footage. Had they done so this would have revealed the identity of the fraudsters.

As no agreement could be reached the matter has come 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.

I would add too that our rules allow us to receive evidence in confidence. We may treat evidence from banks and financial businesses as confidential for a number of reasons – for example, if it contains security information, or commercially sensitive information. Some of the information Amex has provided is information that we considered should be kept confidential. This means I haven't been able to share a lot of detail with Mr S, but I'd like to reassure him that I have considered everything.

*The disputed payments out of Mr S's account*

Between 30 April and 5 May 2023, twenty payments totalling just under £64,000 were made from Mr S's account. Mr S says he did not authorise these payments. Based on what he's told this service and Amex, he is suggesting that an unknown third party was able to make these payments without his knowledge or consent.

There are regulations which govern disputed transactions. Generally speaking, if the evidence suggests its more likely than not that Mr S authorised the payments, (either by making them himself or allowing someone else to) Amex is entitled to hold him liable for the disputed transactions. The relevant regulations, to this effect, are the Payment Services Regulations 2017 (the PSRs 2017).

The PSRs 2017 say a payment transaction is regarded as authorised if the payer has given consent to the execution of the payment transaction. If a payment service user (customer) denied having authorised an executed payment – the payment service provider (in this case Amex) has to prove the payment transaction was authenticated. And if it is deemed that a payment transaction hasn't been consented to, it isn't authorised.

PSRs 2017 goes onto say a payment service provider is expected to refund the amount of an unauthorised transaction to the payer – subject to some caveats, such as where the payer has acted fraudulently.

Mr S says he didn't consent to or authorise the payments and is seeking a refund of the payments made from his account. Amex say the evidence suggests the transfer and

payments were made by Mr S, and he is therefore liable for them. So, I need to think about whether the evidence I have suggests the payments were authenticated and whether it is more likely than not Mr S, or somebody without his knowledge or authority, carried out the transfers and payments Mr S is now disputing.

Having looked at all the evidence, which includes the technical evidence provided by Amex, I don't think it's unreasonable for Amex to have concluded that Mr S more likely than not authorised the transactions. I say this because:

- Mr S has said that he hasn't disclosed his banking PIN or security banking credentials to anyone else. And he has said that he hasn't lost his mobile phone.
- All but one (the £24,000 payment to A) of the disputed payments were authorised using Mr S's Amex PIN.
- Amex has given me technical evidence to show that Mr S's correct PIN was used to authorise all but one of the disputed transactions.
- Mr S has said that he either lost his wallet or it was stolen sometime between 25 and 29 April 2023. He's explained that he had three wallets and rarely used the wallet where he kept his Amex card. However, I find it odd that if a thief/fraudster had managed to gain possession of Mr S's Amex wallet that they didn't then make use of Mr S' other bank card – an account which at the time held a balance of around £2,000. I also haven't seen any evidence that Mr S reported his Amex card stolen.
- If I were to accept that someone unbeknown to Mr S carried out the disputed transactions, after taking Mr S's wallet, I would then need to think about how they knew the PIN. And quite a bit of his personal information such as his company information and that he used to have an account with C.
- Mr S has said someone must have seen him entering his PIN when he used his card. He's also suggested that fraudsters must have discovered his PIN via Amex. And that his email account was hacked.
- Amex says its records don't show a new PIN being ordered which would mean the PIN used for Mr S' card was still in use.
- I can see that Mr S last used his Amex card on 25 April 2023 in a store for a transaction of just over £130.00. If I accept Mr S's suggestion that he was shoulder surfed by a fraudster on this occasion, they would then have had to physically take Mr S's wallet containing his Amex card without him being alerted.
- I'd also need to accept that a fraudster would have waited until 30 April 2023 to start using Mr S's card. And then carry on using the card over a number of days. There's no plausible explanation for why a thief would do this. I say this because they would have needed to have known or being very reassured that Mr S wouldn't discover his wallet and Amex card was missing and that he wouldn't be checking his email or mobile phone. And discovered the fraud.
- There's also no plausible explanation for why an unknown third party stopped stealing money when Mr S still had an available balance to spend.
- Amex has also provided technical evidence that it sent notifications to Mr S's registered mobile device, which is the same mobile number Mr S has provided to this service, to approve the transactions which were carried out on 3 May 2023 for £85.00 and £1,678.
- The transaction to A was also confirmed as genuine after a push notification was sent to Mr S via Amex's online MYCA app. The user would need Mr S's MYCA ID and password (or his biometrics if this was setup on his phone), plus multifactor authentication where a one-time passcode is triggered to a known email/phone

number.

- Amex has provided technical evidence that the MYCA app was accessed using Mr S's mobile device and the transaction to A was approved as genuine.
- So, I'm satisfied from Amex's technical evidence that Mr S's previously registered mobile device was used when the disputed payment to A was made, and that the payment was authenticated as Mr S's correct security details were entered to access the online MYCA app.
- Mr S says he hadn't lost his mobile phone and no one else had access to his phone. So, there's no reasonable explanation for how an unknown third party would be able to gain access to Mr S's online MYCA banking via his device to carry out the disputed transactions from his account to A or the transactions that were carried out on 3 May 2023.
- Mr S says he was elsewhere when the disputed transactions took place. And he's provided photographs and invoices to support his explanation. That may be the case. But that doesn't mean the transactions weren't carried out without Mr S's knowledge or consent by someone else.
- Mr S has said that an unknown third party was also responsible for the transaction carried out at C. And that fraudsters worked out that he was an owner of a business and took a chance that he used to have an account with C. Mr S has also suggested that staff at C must have been complicit to facilitate the gold bullion transaction. I've thought about this and having done so I think this is unlikely. I say this because there's no plausible explanation for how anyone other than Mr S would have known he used to have an account with C.
- The disputed transactions reduced Mr S's available account balance. Amex has provided technical evidence that it sent Mr S alerts to his mobile phone. I also note that Amex sent alerts to Mr S's mobile phone on 5 May 2023, following declined transactions at C for £26,699.99. So, given what Mr S has said about still being in possession of his mobile phone, I think he would've noticed the transactions much sooner than he's said he did as his available account balance was reducing. So, I think if he hadn't authorised them, he would've raised this with Amex at the time. But he didn't alert Amex until after the 17 May 2023, which was well after the *last* disputed transaction was made.
- I note that Mr S has said that someone other than him contacted Amex to gain access to his account. I've listened to all the available calls – in particular a call made by an individual on 5 May 2023, who verified themselves by providing Mr S's father's date of birth. The caller told Amex they were trying to make a purchase and it had been declined. I can see from looking at the technical evidence that Amex had sent an alert to Mr S's mobile phone to let him know it had declined further transactions at C. So, I think this alert prompted the call.
- I've already said that I think it's likely Mr S authorised the disputed transactions. So, I don't need to make a finding on whether it was Mr S who spoke to Amex on 5 May 2023. But for the sake of completeness, I think this call shows someone with access to Mr S's phone – or in possession of personal information about him – knew about the transaction.
- Mr S has also said that Amex should have recovered CCTV. And had they done so it would have revealed that Mr S hadn't carried out the transactions. But retailers only keep CCTV for a relatively short time, so it's rarely useful in disputes like this. Even if a transaction is made by a third party, it's always possible an account holder has asked someone else to carry out the transaction on their behalf. So, CCTV would be very unlikely to help with the outcome here.

I recognise that Mr S has said that he didn't authorise the payments. But based on the evidence I've looked at it's hard for me to see how an unknown fraudulent third party could have obtained all of Mr S's security information, his Amex card and PIN and his mobile device to authenticate the payments. When I weigh everything up, on balance, the most likely explanation here is that Mr S made the disputed transactions himself or allowed them to be made.

*The closure of Mr S's account and customer service*

I've considered whether Amex acted fairly in closing Mr S's account. I've looked at the terms and conditons of the account and I'm satisified it did.

The terms and conditions outline that Amex can close a customer's account with two months notice, and in certain circumstances it can close an account immeidately. In this case Amex closed Mr S's account without notice. For Amex to act fairly here it needed to meet the criteria to apply the terms for immediate closure. And having looked at these terms and all the evidence, I'm satisfied that Amex has applied the terms fairly. It follows that Amex was entitled to close the account as it did.

Finally, I can see that Amex has accepted it fell short on the service it provided to Mr S because it took longer than its agreed timeframe to respond to Mr S's fraud claim. Amex has apologised and offered Mr S £50 compensation. I think this is a reasonable and fair offer. So, I won't be asking Amex to do anything more.

In summary, I know this will be disappointing for Mr S, but with everything I've seen I'm perusaded that the transactions Mr S dipsutes were most likley authencitcated and consented to. That in turn means hey were authroised and Amex are axcting failry by holding Mr S liable for them.

**My final decision**

For the reasons I've explained, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 25 March 2025.

Sharon Kerrison
**Ombudsman**