DRN-3587132

The complaint

Mr X complains Santander UK Plc ("Santander") has refused to refund him around seventy disputed transactions made from his account. Mr X also complains Santander have unfairly withheld his remaining funds.

What happened

Mr X is professionally represented, but to keep things simple I will refer, where possible, to 'Mr X' going ahead.

Mr X opened his Santander account in 2014. Between August 2018 and early October 2018 over seventy separate transactions were made from Mr X's account which he says he didn't authorise. These transactions amount to around £200,000 and are mainly made up of card payments with some cash withdrawals.

At the time these transactions were made, Mr X says he was abroad, and his visa to travel to the UK had expired – he is not a UK citizen. Mr X has a property in the UK, which he owns and resides in. Mr X has a daughter who is living and studying in the UK. She lives at a different address in the UK to that of Mr X.

Mr X says no one was living in his UK property at the time the disputed transactions took place. Amongst other things, he says he only started to discover what had happened when his cheque, made out to his daughter, bounced in October 2018.

Mr X called Santander around this time and was told he would need to come to the UK and visit one of its branches with identification before it could do anything more to help him.

Santander had blocked Mr X's account in October 2018 after reversing two payments as it had become suspicious about some of the transactions.

Mr X renewed his visa and passport and travelled to the UK in August 2019. It's at this point Mr X says he became aware of the transactions. He says he was shocked to learn about what had happened, and he had not authorised anybody to carry them out.

Santander did not uphold Mr X's claim. In summary, Santander said:

- The new card and PIN used to facilitate the disputed transactions on Mr X's account were sent to his residential address

- Santander were able to locate a call in which these credentials were ordered, made from the landline telephone number registered at Mr X's address. As Mr X hasn't been able to provide any evidence of unauthorised access to his property it can only conclude access was given to a third party

- This is further supported by the fact that despite Mr X's claim his property was unoccupied since 2016, he continued to use direct debit to pay for telephone, energy and gas services

Mr X referred his complaint to this service. One of our Investigator's looked into the complaint - they did not uphold it. They made several findings which are known to both parties, so I won't reiterate them here.

In response, Mr X's representatives made the following points:

- The phone provider has confirmed no call was made from Mr X's landline (to order the new card and PIN). So it is incomprehensible there was explicit authorisation by Mr X

- To conclude Mr X gave authority to a third-party, rests on the assumption the new card and PIN were ordered from his home telephone number, which it was not

- Santander did not investigate this matter under its obligations under the FCA's DISP complaint handling rules

- The Investigator has relied on evidence which hasn't been inspected. That's because she had not been able to view electronic evidence to show the card transactions were authenticated but thought it reasonable to suggest they were. This is concerning and should be reviewed

- Mr X's bank statements will show he's never used online banking. This key piece of evidence has been ignored

- Santander should be able to trace the IP address of any device used to find who has made the transactions – but its failed to do so

- The transactions cover a wide geographical area. Mr X was abroad in a different country, and unable to travel to the UK as his passport and visa had expired. If transactions were authenticated using CHIP and PIN, the card must have been shared amongst various individuals or somehow duplicated. There are many possibilities. This is something that must be investigated to determine authentication

- It's unrealistic to say any items fraudulently ordered were delivered to Mr X's address. It's not necessary for someone to have access to Mr X's home to receive any post. Any post could have been delivered to a mailbox, door slit or left on the ground

- It's also plausible the card and PIN never reached Mr X's address or was intercepted

- No guilt should be placed or inferred upon Mr X's daughter without a formal police investigation

- The landline could have been spoofed – a method used by professional scammers

- There are several known methods to overcome security questions. Personal security information is easily obtainable by fraudsters through fake job listings and fake forms being sent to individuals. This information can then be used to pass bank security.

  It's also possible that information may have been passed from someone inside Santander to the fraudster

- The statements were not sent right after the payments were made so Mr X could not have been alerted. Because of this, Mr X questions why his statements were not sent

- A phone recording of the person ordering the card and PIN must have been provided by Santander and should be reviewed. This would show a data breach likely occurred

- As there were no signs of a break-in, nothing was previously reported to the Police. Mr X and his daughter were both told to not contact the Police by Santander. There must be some record of this. Mr X has now reported the fraud to the Police

- There's enough evidence to lead an investigation to the true perpetrators. For example, tracing matters back to the merchants and tracing funds through the banking system. The investigation therefore hasn't been comprehensive enough nor diligent

- Mr X has never used his card for the account. The card he had couldn't be used as it had expired. No details of the phone number used to call Santander have been provided

- It's unsafe to conclude a call made in August 2018 to authorise and verify payments was Mr X without having listened to Mr X's voice and compared the calls

- Mr X's remaining funds are still being withheld and blocked by Santander

- Santander should have internal safeguards to prevent this sort of fraud

The complaint was then passed to me to decide. I then sent both parties my provisional decision. I said that I was not planning to uphold Mr X's complaint. For ease of reference, I've added it here:

My provisional 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 that, I'm planning not to uphold Mr X's complaint. I know this will disappoint him, so I'll explain why.

I note Mr X feels strongly about his complaint and questions why some assumptions have previously made by our Investigator. It's important I explain that where I don't have conclusive evidence or where information is missing, I can make my decision based on what I think is most likely to have happened – the balance of probabilities.

Authentication

This is effectively the process by which a bank should demonstrate that it followed its own internal process and proper form to authenticate a payment. To that end, it's broadly typical for technical records to be kept that show the CHIP and PIN was used, or the online security protocol was met to authenticate a payment.

Santander have been able to send me technical records that show where online or mobile banking were used, the security protocols were correctly passed, and any payments made were authenticated in line with its processes. Similarly, where certain additional security measures associated to card providers were required, these were also correctly authenticated.

However, that doesn't deal with most of the transactions which were made by card payment and cash withdrawal. Santander does not have the technical records for this given the time that's passed since the transactions took place. This of course is unfortunate. Mr X says making a finding on this point without that information is unsafe.

As I've said above, where information is inconclusive or isn't available, I can make my decision on what I think is most likely to have happened. All these payments were made using the card and were done so in 2018 – whether that be online or physically. In 2018, it was industry practice, as it is today, that any physical payments are completed using CHIP and PIN. That would also be the case with ATM cash withdrawals.

Any payments made online would also have required knowledge of the card details – for example the long number on the front, expiry date and CVV number on the back. So given these details would most likely have been needed, I'm persuaded on balance, that these transactions were most likely authenticated in line with the Santander's internal security process and met its proper form.

I note Mr X's representatives say that as the transactions cover a wide geographical area, the card must have been shared amongst various individuals or somehow duplicated. In broad terms we have not seen enough evidence to show a card's CHIP can be cloned.

Importantly, in terms of reaching a finding on the authentication point, I need to determine if I think the proper process to authenticate a payment was followed – and I've already said I think, on balance, it most likely was.

Consent

But the regulations relevant to this case say that is not, on its own, enough to enable Santander to hold Mr X liable. So I also need to think about whether the evidence suggests it's more likely than not Mr X consented to the transactions being made. Any finding here is crucial to the outcome, and to that end, is the crux of Mr X's complaint.

Did Mr X consent and authorise the transactions himself?

I've seen a copy of Mr X's previous and latest passport which show it had expired during the time the transactions took place in 2018. I've also seen his UK visa had expired and was only renewed just before he came to the UK to visit Santander's branch in 2019. So, I'm persuaded Mr X wasn't in the UK.

In saying this, I considered why he was paying for utility, television and telephone services for his UK home if he – or no one else – was living there. But Mr X says he travelled for business, and so I can imagine he wouldn't have always known when he'd be in the UK - especially as he is not a UK national. Given the sums Mr X held in his account, I can also understand why he may have been more than tolerant to pay for services he wasn't always using.

So, to conclude, I'm satisfied Mr X wasn't in the UK when these transactions were carried out. Given the new card and PIN would have been received in the UK and most of the transactions carried out here, I'm persuaded Mr X didn't physically carry them out himself.

Did Mr X give someone authority to carry out the transactions?

Mr X has sent me telephone bills which show no calls were made around summer 2018. The phone provider too has confirmed that no calls were made in July 2018 when the card and PIN were ordered. Santander haven't given me any information to show someone called it

from Mr X's landline in July 2018 to order a new card and PIN. So, I'm satisfied Santander was wrong to say a new card and PIN were ordered from Mr X's landline number.

Because of this I don't think its likely Mr X's landline number was spoofed – but more likely a different number was used. So Mr X's argument about his number being spoofed isn't something I need to consider further.

But Santander have sent me its internal records which show a card and PIN were ordered in July 2018 and they were sent to Mr X's address. I note Mr X says letters could have been sent to a mailbox, left on the floor, or put in a slit.

It's common practice for banks to send new cards and PIN numbers in separate envelopes. Mr X hasn't sent me any compelling evidence to show he was having problems with receiving his post. I've also listened to a call Mr X had with Santander in September 2019 when reporting the transactions. Amongst other things, he says that when he did come to the UK there were lots of letters on the floor – but none from Santander as his account was under review and blocked.

So, despite the landline not being used to order a new card and PIN, I'm satisfied from what I've seen they were likely sent to Mr X's address and that it was most likely correctly posted and delivered. In reaching this finding, I've also considered if the post was possibly intercepted. But I haven't seen any evidence to suggest this is what likely happened.

Mr X has said there's no evidence of a forced break-in at his UK home. In a call to Santander in September 2019 he said no one had a key to the property other than himself. His representatives later said his daughter had a key – but never had reason to visit the property. Nor did his wife, who would stay with the daughter when in the UK at her address. I'm satisfied the daughter lived at different address given the information I've been sent.

I do question why Mr X has been discrepant and inconsistent about no one else having a key – and then later saying the daughter had one. Mr X has since explained the daughter having a key was a backup should he forget to bring his to the UK. He also explains she used this to check up on the house when her cheque bounced and that's when they discovered no bank statements were being delivered.

These are all plausible explanations and they sound like sensible steps to take. What I do struggle with however is how unauthorised individuals would have had access to the house to acquire the card and PIN, which would have been sent on separate occasions, knowing they could be caught in the house at any time.

After all, they wouldn't know if Mr X, or his family, were not going to be there. So there is a serious risk of being captured. That in turn makes me think that anyone carrying this out had detailed knowledge of Mr X and his family's whereabouts, and their plans.

The other aspect of this complaint that makes me think someone knew key information about Mr X that he ought only to know himself, is the ordering of the card and PIN, and the setting up of online and mobile banking. Mr X is clear that he never shared his personal security information with anyone. So it's difficult to understand how someone would have known these details without Mr X telling them.

I've had no plausible explanation as to how this information may have come into the hands of a fraudster. Mr X has said there are several known methods to overcome security questions. For example, personal security information is easily obtainable by fraudsters through fake job listings and fake forms being filled out by potential victims. He adds that it's

also possible information may have been passed from someone inside Santander to the fraudster.

I accept that the above explanations are possibilities, but there could equally be other explanations. Importantly, I haven't seen any evidence to show Mr X was duped into giving out his personal information nor that someone within Santander passed this information on to a fraudster.

So, given what I've said above, I find it difficult to understand how an unauthorised individual would have known Mr X's personal details to not only order a new card and PIN, but also set-up online and mobile banking, without some complicity from Mr X. This is further supported by there being no persuasive argument to explain how a fraudster would have had access to Mr X's property, over at least two separate visits.

I have been able to listen to the call made to Santander in August 2018 shortly after a block was put on the account. And I've listened to the call Mr X made in 2019 when discussing the transactions with Santander's fraud case handler. Mr X doesn't dispute having a phone conversation with Santander in 2019, but says it wasn't him that called in 2018 to lift a block on his account.

In the 2018 call, the individual passes security seamlessly and even confirms two digits of a personalised security code. They also confirm Mr X's correct landline. They also confirm card transactions which led to the block to validate them. Mr X has argued that Santander ought to have done more to safeguard him from fraud. This is a measure it took.

Having listened to the 2018 and 2019 calls, I'm satisfied they are not the same person. So I think our Investigator was wrong to say they were. But they were not able listen to the call, which I subsequently have been able to.

Though the two people on the calls are most likely different people - despite sounding demographically similar - this doesn't mean an unauthorised individual carried out fraud against Mr X. For the reasons already given, I still think its most likely Mr X authorised someone to act in his stead given the knowledge required of personal security information and access to the home.

Having listened to the 2019 call Mr X had with Santander's fraud case handler; I note he is asked whether he has reported the matter to the Police. Mr X says he is not prepared to go to them as the matter is one for Santander to deal with for not protecting his funds.

Mr X says both him and his daughter were told not to contact the Police by Santander. I've carefully read the internal records Santander have sent me, and I can't see anywhere they were told this.

I do question why Mr X didn't go to the Police immediately after he became aware of what had happened. But I'm not placing too much weight on this point as an indicator of whether Mr X did or didn't authorise someone to carry out the transactions in dispute here. That's because even if he didn't want to call the police as I've heard him say, there could be reasons for this – including what he's said. That is, he felt it was Santander's role to investigate the matter and put things right.

Mr X says account statements were not sent right after the payments were made. So they didn't alert him to what was going on. From what I've seen, I think the statements stopped being sent once the account was blocked for review in September 2018. But I don't think the point Mr X is making would have made any difference. That's because he wasn't in the UK

and he's said no one else was in the house up until his daughter went there later after her cheque bounced. The account was already blocked at that that point.

Mr X says he never used his card nor online or mobile banking. Having looked at the account activity I have no reason to disagree. But this, in of itself, doesn't indicate Mr X didn't authorise someone to carry out the transactions by giving them his personal details and access to his home.

Mr X says Santander has failed in its obligation to investigate this matter properly. He says that knowing IP addresses, and where and to whom payments were made to, should be enough information for Santander to trace the fraudsters. There are ways to circumvent IP addresses. Also, the level of investigation required, and legal powers needed to be as comprehensive as Mr X suggests is likely best suited to the Police.

I note Mr X's daughter had a key to his house. To be clear, I make no finding on this point or the argument put forward that it doesn't mean she was complicit in any fraud.

Santander don't have the recording of the call made in July 2018 to order the new card and PIN. That is unfortunate, so I've relied on the evidence I do have when reaching my decision.

So, after having weighed everything up, I've decided it was most likely Mr X authorised someone to act on his behalf and carry out transactions he now disputes. That means I'm persuaded he authorised the payments. So Santander is not liable to refund them to him.

Account review and closure

Banks in the UK are strictly regulated and must take certain actions in order to meet their legal and regulatory obligations. They are also required to carry out ongoing monitoring of an existing business relationship. That sometimes means banks need to restrict, or in some cases go as far as closing, customers' accounts.

Given the nature of the activity on Mr X's account, and the concerns Santander had, I think it acted fairly when reviewing and blocking the account.

A bank is entitled to close an account just as a customer may close an account with a bank. But before a bank closes an account, it must do so in a way, which complies with the terms and conditions of the account. And in certain circumstances it can close an account immediately or with less notice. Having reviewed the account terms, I'm satisfied Santander acted fairly when deciding to close Mr X's account.

Mr X says his remaining funds are still being withheld by Santander. Having seen the reasons Santander has done this, and given the obligations it must adhere to, I don't think it is acting unfairly by holding the funds. I'm under no obligation, that I'm aware of, to disclose these reasons"

The deadline for responses to my provisional decision has now passed. Santander agreed with what I said and made no further representations.
Mr X's legal representative's disagreed. To keep matters simple, I will summarise the key arguments here. But before I do that, and to be clear, I will only address points which relate to findings I made – not any the Investigator reached before the complaint was passed to me.

When a complaint is passed to me for decision, I look at it afresh and independently.

Summary of response from Mr X's legal representative

- Caution should be exercised in the determination of an assessment to avoid assumptions unless there is a *proper* inferential basis for such a conclusion

- The Ombudsman has effectively said Mr X is being disingenuous by concluding he passed his personal security details to a third party. This conclusion is flawed and doesn't properly exclude all other potential scenarios including Santander's failure to prevent the activity

- From the time the account was opened in 2016 up until the disputed transactions in 2018, the account activity shows expenses were only paid by direct debit and cheque. No purchases were made by debit card or on-line banking. This is consistent with Mr X using the account as a deposit one for the purpose of meeting direct debits and his daughter's fees.

  The disputed transactions are clearly unusual given the pattern beforehand. This type of behaviour is consistent with card fraud whereby fraudsters dissipate funds through the purchase of high value items such as jewellery. The only logical conclusion that can be drawn is that Mr X was not using the card and was a victim of fraud

- Given Mr X's age, previous spending history and the unusual nature of the fraudulent spending, Santander's anti-fraud control system should have flagged it. Santander has a legal requirement to have such a monitoring system designed to identify unusual activity with automated service contact.

  Santander says it has such a system in place, but it was not properly engaged in Mr X's case. Substantive sums being paid to high end jewellers is indicative of fraud, and Santander's systems failed to identify this. So Santander failed in preventing fraudulent transactions on Mr X's account – it did not properly or forensically look at the transactions.

  The Ombudsman has failed to consider how Santander's anti-fraud systems failed to pick up the transactions, and by doing so, its failed to meet its legal requirement.

  The changes in Mr X's account behaviours should have triggered Santander's systems. Mr X's representative has highlighted several transactions which they think should have triggered Santander into checking their authenticity.

- Santander falsely asserted it had the call from July 2018 when Mr X called from his landline to order a new card and PIN. This raises significant questions about the validity and reliability of its anti-fraud systems in place at the time.

  Santander falsely assumed Mr X had called them as security had been passed, and this error meant it failed to follow other lines of enquiry and investigation. No call notes been provided.

- Both Santander, and this service, have falsely put the burden on Mr X to show there was unauthorised access to his property

- Despite the Ombudsman concluding calls provided by Santander from 2018 and 2019 of purported calls with Mr X, were not the same person, the Ombudsman has said the only conclusion is that Mr X gave authority to the ultimate caller

- There has been a failure to consider sections 75-77 of the Payments Service Regulations 2017, which says the burden rests on the payment service provider to demonstrate transactions are authenticated, accurately recorded, not affected by technical breakdown or some other deficiency.

  As Santander did not have the technical records, the Ombudsman said it's reasonable to conclude the transactions were authenticated by CHIP or PIN, a contactless feature or the correct card details were used online. But this conclusion doesn't consider Mr X could have been the victim of a sophisticated fraud. This is supported by Mr X's landline not being used to make the call in which a new card and PIN were ordered as previously asserted.

  The absence of Santander's technical records shouldn't be held against Mr X. Where information is inconclusive or unavailable, to then say Mr X authorised the transactions, is too easy a line to draw.

- As Mr X wasn't in the UK, no one had access to his home, and the order for a new card and PIN wasn't from the landline, there has been a failure to consider that the fraud was perpetuated by employees of Santander. The burden is on Santander to prove its security was 'water-tight' and no such internal compromise occurred here.

  There are well publicised examples of such fraud being committed with a similar spending patterns and items purchased to that of Mr X's account. And why would Mr X seek to defraud himself whilst out of the country

- Santander hasn't made requests to trace the transactions, particulars of the payees by seeking CCTV or other identification evidence. Instead, Santander has assumed Mr X gave permission for the use of his card

- The Ombudsman has failed to consider Santander hasn't given any information to show what enquiries and investigation it carried out.

  There's no information which shows Mr X's security information wasn't compromised by Santander. It would have been possible for Santander's fraud team to have traced payments, locations, IP address, and sought to discover where valuable items were purchased and seeking CCTV recording from the retailers. It would appear the only line of enquiry has been the security protocols for the payment.

  This line of enquiry without additional investigation will always stop at verification. It then reverses the burden making the complainer having to prove they did not provide his security details.

- Mr X's failure to report the matter to the Police does not add weight to the suggestion he had something to hide.

- Mr X's remaining funds should be returned to him. No AML concerns were raised by the time of the deposits.

As both parties have now responded, I must now decide this complaint.

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 having 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 Mr X 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.*

Regulation 75 of the PSR also explains:

> *75.—(1) Where a payment service user—*
>
> *(a) denies having authorised an executed payment transaction; or*
> *(b) claims that a payment transaction has not been correctly executed,*
>
> *it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the payment service provider's accounts and not affected by a technical breakdown or some other deficiency in the service provided by the payment service provider.*
>
> *(2) If a payment transaction was initiated through a payment initiation service provider, it is for the payment initiation service provider to prove that, within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment initiation service.*
>
> *(3) Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, including a payment initiation service provider where appropriate, is not in itself necessarily sufficient to prove either that—*
>
> *(a) the payment transaction was authorised by the payer; or*
>
> *(b) the payer acted fraudulently or failed with intent or gross negligence to comply with regulation 72 (user's obligations in relation to payment instruments and personalised security credentials).*
>
> *(4) If a payment service provider, including a payment initiation service provider where appropriate, claims that a payer acted fraudulently or failed with intent or gross negligence to comply with regulation 72, the payment service provider must provide supporting evidence to the payer*.

The PSR's define "authentication" as: *a procedure which allows a payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials.*

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 that, I've decided not to uphold this complaint. I know this will disappoint Mr X, so I'll explain why.

Authentication

I said in my provisional decision that as *"these payments were made using the card and were done so in 2018 – whether that be online or physically. In 2018, it was industry practice, as it is today, that any physical payments are completed using CHIP and PIN. That would also be the case with ATM cash withdrawals.*

Any payments made online would also have required knowledge of the card details – for example the long number on the front, expiry date and CVV number on the back. So given these details would most likely have been needed, I'm persuaded on balance, that these transactions were most likely authenticated in line with the Santander's internal security process and met its proper form"

Mr X's representatives argue the absence of Santander's technical records shouldn't be held against Mr X. Where information is inconclusive or unavailable, to then say Mr X authorised the transactions, is too easy a line to draw.

Firstly, the PSR's say authentication isn't in of itself enough to say a consumer authorised a payment. To do so I need to consider if the consumer *consented* to them as well.

I note it is incumbent upon a financial business to prove, within its sphere of competence, the transactions were authenticated, accurately recorded and not affected by a technical breakdown or other deficiency. But Santander no longer hold this information.

So this means I must make a finding on what I think is most likely to have happened. Even if I were to apply the lowest standards a business is expected to have in place to authenticate any payment, for the reasons I've already given in my provisional decision, I still think they most likely were.

In reaching this determination, I've also weighed up the online and mobile banking transactions were properly authenticated and evidenced. And, I haven't seen anything to suggest Santander had issues which meant its card payment authentication protocols weren't effective around that time.

I've then closely considered whether Mr X consented to the payments – especially as I've said, authentication, in isolation, isn't enough to determine authorisation.

Consent

I already accepted the transactions in dispute were out of character to Mr X's previous account behaviour. But before I examine whether I think Santander should have done more to protect Mr X from financial harm, I need to consider whether I think he likely consented to

the transactions.

Mr X's representatives argue that I have failed to consider other scenarios in which Mr X would have been the unwitting victim of fraud committed against him. One such scenario they've put forward is Mr X could equally have been the victim of insider fraud. That is persons working for Santander may have orchestrated the fraud.

This, alongside other sophisticated fraud scenarios, could explain what happened. But I must reach my decision on the information I have – and consider what I think is most likely to have happened.

As it stands, I can't explain how an unauthorised person(s) would have known secure and confidential information - which Mr X says he hasn't divulged to anyone. And, were then able to pass Santander's security protocols to order a new card and PIN, set-up online banking, and collect and access these credentials from his residential address in the UK without some degree of complicity from Mr X.

I note Santander don't have the 2018 call in which a new card and PIN were ordered. But I'm persuaded, that its most likely, security details would have been required by Santander's staff to process this request. I can't of course be sure, so I'm making this finding on the balance of probabilities.

This leads me to decide – on balance – that its most likely Mr X authorised a third party to carry out the transactions. I haven't seen any plausible or persuasive evidence, relating directly to Mr X's complaint, which suggests he was the victim of insider fraud by Santander's staff.

I note Mr X's representatives feel I've falsely put the burden on him to show there was unauthorised access to his property. But he's said there wasn't any signs of forced entry and that only he, his wife and daughter had access to it. So given someone else accessed the property to collect two separate letters containing the card and PIN, I still think its likely he authorised someone to do this.

I've already said the 2018 caller and Mr X were different people. But that doesn't mean Mr X didn't give authority to that person to act in his stead. What I struggle with is how this individual knew enough information about Mr X to have passed its security checks. I haven't seen anything which shows Mr X's personal security details were compromised.

So, weighing everything up, I think, on the balance of probability, Mr X most likely gave someone these details. It's important to remember that I can't be completely sure about this, but my finding on what I think is most likely to have happened is drawn on the information I do have.

That brings me onto Santander's monitoring of the account and whether it failed to protect Mr X from financial harm. I agree financial businesses, like Santander, have an obligation to protect its customers by having adequate anti-fraud monitoring systems in place. But given I think Mr X most likely authorised someone to carry out these transactions, I'm not persuaded how any such intervention would have made a difference. In fact, when Santander did block the account to check the validity of some transactions, the caller was able to pass security and validate them.

I note Mr X says the spending behaviour was strongly indicative of fraudulent behaviour and questions why he would commit fraud against himself if he was outside of the country. I agree the transactions are suspicious in nature and seem to be designed to dissipate the funds rapidly. But I've had to consider how these transactions were likely authorised, and

I've already said its most likely that Mr X was in some way complicit and therefore likely authorised someone to carry them out. I don't think Mr X being outside the UK gives any indication to whether he did or did not do this.

Mr X's representatives say Santander hasn't done enough in relation to gathering relevant information like particulars of the payee, IP addresses or CCTV footage. I'd already said in my provisional decision there are ways to circumvent IP addresses. Also, the level of investigation required, and legal powers needed to be as comprehensive as suggested is likely to be best suited to the Police.

I've also said Mr X likely authorised a third party to carry out these payments, so I would expect to see an individual or individuals other than Mr X carrying them out. After all, he wasn't in the UK.

I'd already said in my provisional decision I wasn't placing any weight on Mr X not going to the Police sooner. So I don't need to engage any further with this point.

Account review, closure and withholding of funds

Mr X's representatives say any remaining funds should be returned to him. And that no anti-money laundering ("AML") concerns were raised by the time of the deposits. I've considered this carefully and having done that I won't be departing from what I said in my provisional decision about this.

So, having seen the reasons Santander has withheld Mr X's funds after reviewing and closing the account, and given the obligations it must adhere to, I think it is acting fairly by holding the funds. Neither Santander nor I, are under any obligation, which I'm aware of, to disclose these reasons.

So, in conclusion, I've decided its most likely Mr X authorised someone to make the transactions he disputes, and Santander have done nothing wrong by withholding any residual funds.

My final decision

For the reasons I've given above, I've decided not to uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask X to accept or reject my decision before 10 August 2022.
Ketan Nagla
Ombudsman