complaint

Mr L complains National Westminster Bank Plc (NatWest) won't refund him for transactions he says he didn't make or allow anyone else to make.

background

Mr L is being represented by a solicitor, but for clarity I'll refer to Mr L when referencing information or points made on his behalf as well as from him directly. All events referred to are in 2017.

On 16 May, NatWest issued a letter to Mr L with 60 days' notice of its intention to close his accounts. Mr L says he didn't receive this letter.

On 3 July, Mr L credited his account £80,000 in addition to receiving other funds. Mr L says he'd put these funds aside for an upcoming investment opportunity and moved them to spread his money across accounts to maximise his protection from the Financial Services Compensation Scheme (FSCS).

On the same day, Mr L says he clicked on a link after seeing an advertisement for a webinar about investing in cryptocurrency. He initially said this was via email but has since clarified he believes his son sent him the link from a Twitter advertisement and they may have later emailed him.

Mr L was asked to pay for this via an online banking transfer and proceeded to set up a new payee using his home PC and transferred £40. Mr L disputes nine payments totalling £53,000 made from his online banking to this same payee following this.

The disputed payments were all made using Mr L's online banking and appear to have taken place from a mixture of IP addresses in the United Kingdom and Turkey.

Mr L has provided evidence that he flew outbound via Turkey on 4 July and returned on 10 July. He queried the activity in a webchat on 11 July and in a call on 12 July. NatWest attempted to recover the funds but was only able to recover £880.76.

Mr L has suggested some sort of key tracking malware must have been installed on his laptop and confirmed he took it, along with his card, with him on his trip – he's suggested this may explain the location similarities.

The following are all the online banking payments from this account in the relevant period, they are disputed and made to the alleged fraudster unless otherwise stated:

Date	Time	Amount	Information about the payment
3 July	17:50	£40	Undisputed payment to alleged fraudster IP address 1, UK
	21:32	£3,000	IP address 2, Turkey
	21:53	£2,000	Undisputed payment to third party IP address 1, UK
	23:17	£5,000	IP address 2, Turkey
4 July	00:55	£4,000	IP address 2, Turkey
	16.03	£5,000	IP address 2, Turkey
5 July	17.37	£5,000	IP address 3, UK
6 July	14.46	£6,000	Close variation of IP address 3, UK
7 July	17.32	£12,000	Close variation of IP address 3, UK
11 July	15.15	£10,000	Close variation of IP address 3, UK
	22.29	£3,000	Close variation of IP address 3, UK
	Total	**£53,000**	

Mr L says that when he made a genuine payment of £2,000 to his son on 3 July, he didn't notice the disputed £3,000 payment which had recently taken place.

NatWest initially accepted Mr L was likely the victim of a scam but has since confirmed it thinks he did authorise the transactions. It highlighted that in order to make a payment online, the individual is required to enter a 10-digit customer number, followed by three characters from a four-digit PIN and three from his password. Further NatWest says Mr L is a sophisticated trader who regularly made large payments to and from his account, and normally regularly accesses his account.

The investigator didn't uphold this complaint. She thought Mr L had likely authorised the transactions, either by making some of them himself or allowing someone else to make them on his behalf.

Mr L didn't agree, he made several points – in particular:

- He provided a news article about a man who appears to have the same name as the recipient of Mr L's disputed payments. This man admitted to attempting to blackmail a large company. Mr L asserts that this individual is highly sophisticated and capable of installing undetectable key tracking software.
- He referred to NatWest's duty of care, the Payment Services Regulations (PSRs) and the Contingent Reimbursement Model as part of why he thinks it would be appropriate for NatWest to provide a refunds and compensation.
- He questioned how the last payment took place if it was after he'd reported the fraud in the webchat.
- He explained he has a high net worth with over £260,000 into his account and £240,000 out of the account and so he can't be expected to notice a £3,000 payment.
- He thought the activity including different locations and failed log-in attempts should have appeared suspicious to NatWest.

The matter was passed to me to decide and I asked for more information from Mr L, NatWest and the receiving bank – in particular:

- Further details from both banks about the recovery aspect of Mr L's funds and relevant information about the receiving account.
- Further detail about what Mr L remembers happening at the time
- A copy of the webchat from 11 July where Mr L reported the fraud and confirmation of timings.
- Evidence of the time Mr L's card was cancelled.
- Terms and conditions of the account applicable at the time.
- Shared one of the newspaper links with the banks involved and invited comment.
- Asked NatWest whether it was prepared to reimburse the last disputed payment of £3,000 when it appeared this took place during the webchat where Mr L reported the transactions as fraud.

NatWest confirmed it was not prepared to offer to reimburse the £3,000 on the grounds that it believed he was involved. The newspaper article didn't change its position and it said it was an oversimplification to conclude this third party had obtained his secure information because he was a hacker. Both banks confirmed recovery was sought on 12 July and available funds were returned.

The receiving bank confirmed the account was not newly opened and there were no other reports of fraud in relation to it. Mr L confirmed he first found out about the payments when he returned from his trip and logged into his online banking.

I issued my provisional decision on 3 September 2020, explaining why I didn't intend to uphold this complaint. I said I thought it was reasonable that NatWest had concluded Mr L authorised the disputed transactions.

Mr L didn't agree, he said:

- Malware could have been installed on his laptop on a previous trip without his knowledge. This would have enabled the fraudster to obtain his full online banking log-in information over time.
- He thought the newspaper articles showed the individual at the heart of this fraud committing the same crime.
- Mr L's previous large payments don't mean he authorised these
- He's never allowed anyone to make payments on his behalf – and thinks it's beyond our scope to assume he has done so here
- How and when the payments were made is irrelevant, the loss remains, and he reported it as soon as he was aware.
- Mr L not be held to the standards of a reasonable man, his talents and achievements exceed this – he shouldn't be punished for not noticing a £3,000 payment
- He didn't agree the evidence was inconsistent with his version of events
- That he's entitled to any payments after the webchat or recovered.
- If NatWest had stopped some of the payments, then that would have reduced his loss.

my findings

I've considered all the available evidence and arguments - including Mr L's response to my provisional decision - to decide what's fair and reasonable in the circumstances of this complaint. Having done so I am not upholding this complaint, I'll explain why.

It's important to highlight that with cases like this I can't know for certain what has happened. So, I need to weigh up the evidence available and make my decision on the balance of probabilities. And determine what I think is more likely than not to have happened in the circumstances.

I agree that the PSRs are relevant to this case and think the 2009 version is applicable here. The account terms and conditions are also pertinent – relevant sections say:
"*2.2.1 You authorise us to act on your instructions, even if they create a debt on your account. You are responsible for payment of any debt which arises on your account.*
2.2.2 Your instructions can be given in writing (which must include your signature(s)), by cash machine or, where we agree, by telephone, online, by contactless card, mobile message or by any other means we tell you are available. You must use the security procedures we notify you of from time to time…
2.4 Protecting your account
You must:
(a) keep your PIN (personal identification number) and other security details secret; and
(b) tell us immediately if you think someone else may know your security details or if you suspect unauthorised use of your account…
4.5.5. Where you have:
(a) allowed another person to make payments (other than someone that we have agreed may be allowed to use your account); or … you will be responsible for all payments made in this way before you tell us that any transactions are unauthorised."

The PSRs require a payment to be correctly authenticated and made with the customer's consent in order to be regarded as authorised. Here, *"authenticated means the use of any procedure by which a payment service provider is able to verify the use of a specific payment instrument, including its personalised security features."* (Reg 60)

Consent *"must be given in the form, and in accordance with the procedure, agreed between the payer and its payment service provider".* (Reg 55(b))

NatWest has provided Mr L's online banking records and confirmed its security process. These show his online banking was accessed in line their procedure – using his customer ID, and elements of his secure PIN and password. Mr L has confirmed he previously set up the payee. So, I'm satisfied these payments were correctly authenticated and that the form and procedure agreed between the parties (as set out in the account terms) was completed. But this is not enough to say Mr L authorised them.

Mr L has said there should have been two factor authentication in place for these payments. Whilst Mr L did need to use his card and card reader to set up the payee, once this was done NatWest didn't require this for every payment. It isn't our role to set businesses security procedures – the Financial Conduct Authority is responsible for regulating NatWest – and there was not a requirement for NatWest to incorporate two factor authentication for every online payment in place at the time. But I will go on to comment on NatWest's duty of care later.

Did Mr L authorise the payments?

With the above in mind, I think the key question here is whether Mr L, or someone that can be treated as acting as his agent, made the transactions. I accept Mr L did not physically make all the disputed payments himself – clearly the payments originating from different countries in a short period of time (particularly on 3 July) makes this improbable. And he's shown that he was on a flight for at least one of them. So, I've considered whether Mr L gave someone else his online banking information on the understanding that they would be able to make payments on his behalf. And I think, on balance, that he did.

I say this because:

- There's no persuasive explanation as to how an unauthorised third party obtained Mr L's online banking information. I've considered the possibility, as put forward by Mr L, that his computer was hacked and malware (such as key tracking software) was installed when he clicked on a link. I don't think this is likely given no malware was found on his computer after he reported the fraud and he isn't sure he clicked on a link whilst using that device. But even if a sophisticated fraudster were able to place undetectable malware on his computer, Mr L only logged into his online banking once that day (3 July) before the first disputed payment was made. Only partial secure information is used which changes at each log-in. Here different characters/digits were used to authenticate the log-in for the first disputed transaction from those Mr L had used earlier that day. Further to this, several other combinations were used to log on throughout the disputed payments and so it's likely Mr L's full customer ID, password, and PIN were known. I've gone on to consider his most recent suggestion that malware was installed on his laptop at a previous date, enabling the fraudster to collect this information over time. Unfortunately, there isn't any evidence to support this theory and it doesn't explain how there could be a connection between someone who had previously gained all of Mr L's online banking information and the webinar he chose to purchase.
- Mr L has provided little detail as to how a scam may have unfolded. He hasn't been able to provide a copy of the email he's referred to and has repeatedly confirmed he didn't share his online banking information. I'm also not aware of any police involvement which you might expect given the amount lost.
- Mr L credited the account with a significant amount of money on the day the disputed payments began. I understand Mr L says this was in order to spread his funds across different banks. Whilst this is plausible, the timing of this in light of the other circumstances suggests the deposits were linked to his intention to make payments from this account.
- A £3,000 payment had already been made when Mr L logged on to make a payment to his son. I understand Mr L says he didn't see this and that he has a large turnover in his account. But I don't think this is a small amount of money and he would have seen his balance earlier in the day when making the £40 payment. Mr L is a self-declared sophisticated investor who doesn't use others to help with his finances, so I think it's fair to infer he'd be aware of what funds he was expecting to come in and out of his account. I understand Mr L doesn't agree with this, and feels he is being punished for not noticing this. It isn't our role to punish either party, and it is of course possible he simply didn't see it. But I think it is relevant and in light of the other evidence I've set out, I'm not persuaded he was unaware of this payment.
- The pattern of the payments is inconsistent with that of an unknown fraudster who with full access to Mr L's online banking. Mr L had over £90,000 in his account at the time of the first disputed payment, yet only £8,000 is said to have been stolen in the first day. There are also large gaps of up to three days between disputed payments.

More commonly a fraudster will try to take as much as they can, as quickly as possible, before they are discovered as delay risks their access being blocked. Mr L says that how and when the payments were made is irrelevant. I don't agree; as part of my review into whether NatWest has fairly declined Mr L's request for a refund, I've needed to consider whether it's more likely than not the payments were authorised. This activity is inconsistent with Mr L's assertion that a third party made these payments without his knowledge. If this was the case, the fraudster would have no way of knowing Mr L wouldn't be logging onto his online banking during this time period.

- It's a significant coincidence that some of the disputed payments originated from an area Mr L appears to have connections with – in terms of regularly travelling to the region.
- I've reviewed the news reports provided by Mr L about an individual with the same name as the payee here. In summary these refer to a man who was convicted of attempting to blackmail a large company by making a series of threats about accessing their customer accounts. It's not certain that this is the same man, but more importantly, if I was to accept he was the same person, this wouldn't be enough in itself for me to uphold this case.
- The similarities in the cases are rather loose and relate only to the general nature of his involvement in an attempted cybercrime. I note the reports suggest this criminal had overinflated his abilities and accessed accounts previously compromised in unrelated events. One report says *"The NCA investigation also confirmed the findings of (company name) that there were no signs of a network compromise. The data (man convicted) claimed to have was actually from previously compromised third party."* The facts in these reports are quite different from what Mr L thinks happened to him. And I don't find this persuasive evidence that Mr L was hacked by a highly sophisticated fraudster.
- It would also be unusual for a sophisticated cybercriminal to share his real name with his victims. Here the receiving account was not newly opened and there were no other reports of fraud in relation to the account. Whereas, the subject of the news reports did attempt to keep his identity hidden and appears to have been acting on behalf of a wider group.

I agree that Mr L's history of large payments doesn't mean he authorised these. My understanding is that NatWest would have raised this in relation to whether it ought to have identified the disputed activity as suspicious – I'll go on to address this point separately.

Did any payments take place after Mr L reported the fraud?

I note Mr L's point that the last disputed payment appeared to have taken place after NatWest were on notice that he wanted it to prevent further payments. The investigator was initially informed that Mr L notified NatWest an hour earlier than I now believe to be the case, I'll explain why.

Reg 62 the PSRs say
"(3) of Except where the payer has acted fraudulently, the payer is not liable for any losses incurred in respect of an unauthorised payment transaction -
(a) arising after notification …"

The Webchat records show Mr L beginning the conversation at 22:08 and at 22:25 Mr L wrote *"please don't let any more transfers out".* But when reviewing Mr L's online banking records, I noticed that the IP address he'd previously used for undisputed transactions

wasn't accessed until 23:00 on 11 July. And that all previous log-ins that day originated from the IP address used to make the disputed payments. Given the implications of this I asked NatWest to confirm what time Mr L's card was cancelled – NatWest confirmed this was at 23:30 on 11 July. This correlates with the Webchat which shows the adviser offering at 22:26 to cancel Mr L's card "immediately".

So, I think it's more likely than not that the Webchat records are an hour out. This could be for many reasons and may be linked to some systems, but not all, reflecting the clocks changing for British Summer Time. This would mean the last disputed payment was made before Mr L reported any disputed payments.

For clarity, were I to make the alternative finding that Mr L had reported the fraud an hour earlier, this would be unlikely to impact the outcome here and would provide serious implications about Mr L's involvement in fraudulent behaviour. This is because there would be no explanation for how he'd identified the payments unless he had been colluding with those who made them. So, while it would be clearer if this evidence were more certain, NatWest has accepted this is likely the case and it is not to Mr L's detriment to interpret it in this way.

Is there any other reason it would be fair to uphold this complaint?

My finding is that it is reasonable for NatWest to have concluded these payments were made either by Mr L or someone acting on his behalf. This isn't out of the scope of our Service, rather this determination is central to my consideration of this complaint.

It's possible someone acting as Mr L's agent exceeded the scope of what they had agreed but I have no way to determine this. I don't think NatWest would be liable for an agent of Mr L going beyond their separate agreement with Mr L – any payments would still be authorised until Mr L took steps to remove their authority to act on his behalf by removing their ability to make payments - as he did when he contacted NatWest on 11 July.

Turning to Mr L's points about NatWest's duty of care and the suspicious nature of the activity on the account. I agree that it may well have been appropriate for NatWest to identify some of the activity as potentially fraudulent; there were multiple log ins to Mr L's online banking from different countries in a short period of time, in conjunction with a series of large payments to a relatively new payee.

His previous account activity is relevant to determining at what point the activity would have appeared unusual. In the circumstances I don't think it would help for me to identify the point at which I thought it would be reasonable to expect NatWest to have contacted Mr L to verify the payments. I take Mr L's point that any payments prevented would have reduced his loss. However, I have already found that it was reasonable for NatWest to conclude Mr L authorised these payments. So, without knowing what Mr L had agreed to, it would be completely speculative for me to comment on what would have happened if NatWest had contacted him or to attempt to determine whether this would have made a difference. It's quite possible he would have confirmed they were genuine at the time.

Other points raised by Mr L.

In relation to Mr L's references to the Contingent Reimbursement Model – this was not in place until May 2019 and isn't retrospective, so I don't think it's relevant here.

I've considered Mr L's points in relation to regulations 63 and 64 of the PSRs - refunds for payment transactions initiated by or through a payee. I don't think these are relevant either. The disputed payments were initiated by the payer account via online banking also known as 'push payments' rather than by the payee i.e. 'pull payments', for example a direct debit.

For the reasons explained above, I don't think it would be fair or reasonable to make an award in the circumstances.

my final decision

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 L to accept or reject my decision before 22 February 2021.

Stephanie Mitchell
ombudsman