DRN-4462645

The complaint

Mrs H complains National Westminster Bank Plc ("NatWest") won't refund transactions she disputes authorising due to identity fraud.

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.

Mrs H says she fell victim to a complex identity fraud from around the summer of 2022. She believes her mobile phone, home internet network, and email address had been hacked, which allowed fraudsters to carry out over 300 transactions with various online retailers and a mobile app service provider. The transactions being disputed total over £18,000.

Mrs H says she first reported the fraud to NatWest in August 2022. Mrs H says she cancelled her debit card because of this issue – and she believes one of the newer issues may have been compromised by fraudsters by accessing her post. Mrs H adds that her debit card limit was also increased to around £1,500 without her consent or knowledge.

Mrs H says NatWest failed to alert her of the suspicious activity on her account. And had it done so, NatWest could have prevented her from suffering the financial loss she has. Mrs H therefore feels NatWest has been negligent in its duty to protect her money and account from financial harm especially as her poor health made her vulnerable.

Mrs H has explained in-depth that she was being targeted in various ways by fraudsters which included them stalking her home, observing her at a local café, drones flying next to her home, intimidating messages being sent to her phone and smart television, and receiving silent calls.

Mrs H was also very unhappy with the service NatWest provided her in relation to this matter and how it handled her fraud claim. As a result Mrs H complained. NatWest sent several complaint responses to Mrs H, in which it upheld parts of her complaint. But it didn't uphold Mrs H's claim for the transactions she disputes to authorising.

In summary, some of the key findings NatWest made were:

November 2022 response

- NatWest has reached the correct decision in declining Mrs H's fraud claim. It was declined because the retailers confirmed the transactions were made using a genuine account registered with Mrs H's name and email address. Mrs H would have been made aware of the transactions by email

- Mrs H had also mentioned third party authorised the transactions, so this should be treated as a civil dispute

December 2022 response

- Mrs H hasn't been enrolled for its online banking at all so there is no need to disable this service. NatWest is sorry Mrs H was misadvised about this

- No new bank debit card was sent to Mrs H after she reported the fraud to NatWest on 28 October 2022. Mrs H had asked its agent to not send her another card but just to cancel the existing one. As there is no new card on Mrs H's account since then, no other transactions were subsequently actioned other than her existing direct debits

- There is no limit on a single or daily online transaction. If an online transaction is keyed there is no limit on it. The only limit on the account relates to ATM withdrawals

- NatWest is sorry Mrs H was misadvised in branch that its advisor would get someone to watch her account to ensure its secure. Given the size of its customer base, NatWest would not be able to assign a single person to watch her account. It's Mrs H's responsibility to check all the transactions made on the account are genuine. Because of the misinformation NatWest's agent gave Mrs H, it will be upholding this complaint point

- NatWest is sorry Mrs H didn't receive the level of service it expects from its branch staff. Feedback will be passed to the individuals

- When a transaction is made it receives a risk score, and various factors make up this score. For security reasons NatWest can't divulge what these are. These factors are constantly updated in line with latest fraud intelligence. The fraudulent activity on Mrs H's account didn't receive a high enough risk score to trigger a restriction

- For the poor service Mrs H received and the distress and upset this caused her, NatWest will pay £250 compensation into her account

May 2023 response

- NatWest is sorry its fraud team didn't contact Mrs H within five days of her making her claim

- Mrs H wasn't sent notifications for each transaction made from her account as this preference wasn't turned on. It is down to customers to turn on such notifications on their account. It's the customers responsibility to check their statements and inform NatWest immediately if they don't recognise activity on their account. So NatWest hasn't made any error in notifying Mrs H of fraudulent transactions leaving her account

- Paper statements were turned off on Mrs H's account in 2017. Mrs H had elected to receive them electronically from that point onwards

- NatWest is sorry for the poor customer service Mrs H received from its fraud team. And being erroneously told that someone from the fraud team could meet her in branch

- NatWest's fraud investigator has dealt with Mrs H's claim in line with its processes and expectations. And they reached the outcome to decline the claims following an intensive investigation

- NatWest reached the right outcome in declining Mrs H's fraud claim and it followed

its own process by communicating the outcome over a phone call

- NatWest will not refund Mrs H's travel costs for when she visited a branch as it had not requested her to do so, and the fraud team are a telephony-based unit

- For the poor service Mrs H received, NatWest will pay her £75 compensation

Unhappy with NatWest, Mrs H referred her complaint to this service. I'd like to assure Mrs H that I've very carefully reviewed all the points she has made, even if I don't explicitly set them out in my decision. To avoid repetition, I'll set out the key and novel points she's raised:

- A payment using her debit card was made in a foreign currency. This should have been picked up by NatWest as unusual as she has not been abroad nor used any foreign currency

- NatWest should have opened Mrs H a new account whilst the issue with the fraud was sorted out

- Mrs H went into branch to open a new account but couldn't as she didn't have ID on her nor a debit card. But NatWest should have let her do this as an existing customer and had it done so, she would have been able to transfer funds and not loose them later to fraud

Our Investigator also asked Mrs H about a person she had mentioned to the police who I will now refer to as "K". Mrs H said she had been talking to this individual on an in-game chat and that they had told her they lived nearby. She added that she had never shared any personal details with them only game related information. But seeing that K had their details registered on an online service in her name this has now leads her to believe K might have been stealing from her.

Mrs H explained K had told her they were suffering from cancer. Mrs H reiterated that she doesn't know how fraudsters, including K, carried out the fraud against her. She also explained that she didn't know how some of the online purchase parcels were delivered to her and that she's still waiting for the police to inspect them. Nor did she recall saying that she suspected her partner at any time.

Our Investigator then sent Mrs H their outcome on her complaint. They recommended the complaint isn't upheld. In short, they found:

- Having reviewed everything Mrs H, NatWest and the police have said she told them, there are inconsistencies. Because of the various versions of the events and background, which are mutually exclusive, they can't accurately determine what has happened. Nor can they determine a point of compromise for Mrs H's banking credentials

- The circumstances are unusual for fraud. In that, Mrs H has claimed many transactions with a specific retailer, "E", to be fraud but she sent the transaction history for this retailer which shows they were made through her account with them. And she had told the police she has the parcels from E. It's incomprehensible why a fraudster would do this as they'd expect the parcels to be sent elsewhere for illegitimate gain

- With multiple differing versions of events, and activity that doesn't appear fraudulent, they're not able to find NatWest did anything wrong

- NatWest carried out its investigation based on what Mrs H told it, and this directly contradicted what the police said she told them. Nor do the explanations Mrs H has provided this service explain how someone else accessed her account

Mrs H didn't agree with what our Investigator said. Once again to avoid repetition, I'll only note the novel points Mrs H made in response here:

- Mrs H's complaint centres on NatWest allowing the transactions without alerting her of them. With so many transactions taking place she expects NatWest to have been more proactive especially as she first alerted it in August 2022

- NatWest sends her paper statements which arrives six weeks after the date of the statement leaving ample time for fraudulent activities to go undetected

- Mrs H doesn't believe there are inconsistencies in what she has told this service, NatWest, and the police. The differences are in interpretation. NatWest and the police were working closely together

- The packages Mrs H received are only a fraction of the items ordered

- Mrs H had only answered the police that she would prosecute her partner if he had done it, and anybody else if they had done it. The police in any case had told Mrs H that it wasn't anyone from her household

- The police said there would be different versions from Mrs H given the distressed state she was in

- In December 2023, a new branch manager was horrified to learn a meeting with her, and Mrs H wasn't arranged by her staff. The manager informed Mrs H she had been misinformed about opening a new account because her ID was misplaced. And as an existing customer she could've opened another account to transfer her funds out

- She didn't open a social media account which was linked to her email

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

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 Mrs H 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, banks will be liable for unauthorised payments.

But that is not the end of the story:

- Regulated firms like NatWest are also required to conduct their 'business with due skill, care and diligence' (FCA Principle for Businesses 2) and to 'pay due regard to the interests of its customers' (Principle 6)

And as a matter of good industry practice at the time, I consider firms should also have taken proactive steps to:

- Identify and assist vulnerable consumers and consumers in vulnerable circumstances, including those at risk of financial exploitation (something recognised by the FCA in recent years and by the British Bankers Association's February 2016 report 'improving outcomes for customers in vulnerable circumstances');

- Look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam (something also recognised by the British Standards Institute's October 2017 'Protecting Customers from Financial harm as a result of fraud or financial abuse – Code of Practice', which a number of banks and trade associations were involved in the development of)

This means there are circumstances, irrespective of the payment channel used, where a bank should, in my opinion, fairly and reasonably take additional steps, or make additional checks, before processing a payment, or in some cases decline to make a payment altogether, to help customers from the possibility of financial harm.

This is particularly so in light of the environment created by the increase in sophisticated fraud and scams in recent years – which banks are generally more familiar with than the average customer.

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 Mrs H and NatWest 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've decided not to uphold this complaint. I know Mrs H feels strongly about this complaint and I'd like to assure her that I don't undervalue the impact this has had on her. So, I'll explain why.

I should also note that where evidence is inconclusive or incomplete, I can reach my decision on what I think is most likely to have happened – the *balance of probabilities*.

Did Mrs H authorise the payments?

I'm satisfied from the bank's technical evidence that Mrs H's genuine security credentials were used to make the disputed transactions. So, that means I'm satisfied the transactions were authenticated in line with what the PSR's say. But the PSR's say that is not, on its own, enough to enable NatWest to hold Mrs H liable.

So I also need to think about whether the evidence suggests it's more likely than not that Mrs H consented to the payments being made. Having given this considerable thought, I'm persuaded, that on balance, its most likely Mrs H consented to the payments she disputes. That's because:

- There are substantive and irreconcilable inconsistencies in the testimonies Mrs H has presented to NatWest, the police, and this service. One of the critical issues is that she explained in depth to the police about K and how they may be involved - but she failed to do so to NatWest despite several lengthy interactions.

  The police report details Mrs H informed them that she had met K three years prior to 2022 and she used his E account to purchase an item – though she was clear her card details weren't saved on his account. But I note K's details were also on her account. Mrs H also mentioned to the police that K suspected one of his friend's to have made the disputed purchases and carried out fraud. Mrs H also explained that she had arranged to meet K in a local café. And K had also admitted stealing money from her but later returned it in cash to her.

  None of the detailed fraud, contact and complaint notes I have seen from NatWest show Mrs H explaining K's involvement. Mrs H says this is a matter of interpretation and not inconsistency. But I disagree. Its possible Mrs H was involved in a relationship with someone she met online in a gaming site, and they have taken advantage of her. But the credibility of this position is significantly undermined by Mrs H not explaining this to NatWest and because the payments were from her E account

- I haven't seen any information which shows how Mrs H's details were otherwise compromised for an unknown fraudster to have carried out the fraud. And given the inconsistencies that I've highlighted above, I think its more likely Mrs H shared and therefore gave express authority for someone to make payments on her behalf

- I've also considered that it is highly unusual for any packages ordered online that Mrs H says she didn't authorise payment for to have been sent to her home address. I would not expect a fraudster to behave in this way – at the very least to avoid being detected. Mrs H says that these were merely a fragment of what was ordered in her name, so too much weight shouldn't be put on this argument.

  In isolation this may carry more weight, but given what I've said above, I'm persuaded it only adds more to the likelihood that she gave someone else express authority to carry out transactions from her account

- I've also considered that this individual has taken advantage of Mrs H and made transactions that's he didn't know about. But that is likely apparent authority, and I haven't seen anything to show Mrs H broke the chain of events by removing any authority she conferred upon K

- The Irish fuel company have also said that an account was opened in Mrs H's name with it using her home address and that the computer IP address was from her location. The delivery address and account name were later changed. Mrs H says she never gave anyone her banking security credentials, but this suggests she either initiated the transaction and account herself or gave someone permission and the details to do so

- Mrs H says she has been the victim of a complex and sinister hacking enterprise. But I haven't seen compelling evidence this is the case

Should NatWest have done more to protect Mrs H from financial harm?

I've had a look at the technical information NatWest have provided me of the disputed transactions. Given the small values they start from and how they then gradually intrinsically become part of Mrs H's everyday account activity, I'm satisfied they weren't unusual enough to have alerted NatWest something wasn't right.

Having said that, given I'm persuaded that its most likely, based on the evidence, that Mrs H consented to these payments albeit through express or apparent authority, I can't see how any intervention would have made a difference.

In reaching this finding, I note Mrs H says she told NatWest in August 2022 about fraud being perpetrated against her, so it failed from that point onwards to take adequate steps to protect her. But Mrs H had given NatWest a different version of events to that of the police, and based on what it did know, I'm persuaded it hasn't done anything wrong. I also don't think a single payment to a foreign exchange payment for a sum that isn't unusually high would have alerted NatWest.

I note Mrs H says NatWest failed to open another account for her which she could have safely stored her funds in. But given I think its most likely she consented to the transactions she disputes; I don't think this would make any difference to what happened.

Lastly, I note NatWest paid Mrs H £325 in total for the failings it accepted it made in its customer service provision. It's not clear whether Mrs H is still complaining about this, but in the event that she is, I think NatWest has acted reasonably here. So I don't think it needs to do any more.

My final decision

For the reason above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs H to accept or reject my decision before 27 June 2024.

Ketan Nagla
Ombudsman