DRN-4623748

The complaint

Miss T complains that Revolut Ltd didn't do enough to prevent her losing money to a safe account scam.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here. In January 2023 Miss T says she was the victim of a scam.

Miss T says that a few months prior to the scam taking place, she'd responded to a SMS she believed to be from Apple, she inputted some personal information including some details of her debit card with her bank 'N'. She says she realised soon after that wasn't genuine and she informed N who replaced her card. She thinks that as a result of this, she was later targeted by scammers.

Miss T describes how she was initially called by someone purporting to be from N. She says she was told that her identity had been stolen and that she needed to act quickly to avoid losing her money. The caller said there was a police investigation that had been started. Miss T was asked if she had another account and she disclosed that she also held an account with Revolut. She says she was told that speed was of the essence and that she needed to move her money across to her Revolut account to keep it safe. But before doing so, she should wait for a call from Revolut who were being made aware of the situation by N. She was told that Revolut would be in touch soon.

Miss T was then called by someone who said they were from Revolut's fraud department. Miss T says that she searched the number she'd been called from and that this appeared to link to Revolut (although she later accepted that one digit was different, something she missed at the time and attributed at least in part to her dyslexia). Miss T says she was then talked through moving money from N to her Revolut account. She was then told that the 'malware' had infiltrated her Revolut account and she would need to move the money again into another safe account that was being set up for her within Revolut.

Miss T's letter of complaint records that she was told to share a number from one of the messages received on her phone and that this was needed to 'block her card'. Miss T says she shared the number with the caller. Miss T says she was tricked into sharing the Apple Pay OTP. This allowed Apple Pay to be added to a new device. Miss T says the scammer kept her on the phone and gave her various instructions as to what to do within the Revolut app. She says that she didn't consent to any of the outgoing payments. She realised she'd been the victim of a scam when the last payment left and the scammer never called back.

Revolut were able to recover around £5,750 of the payments that had been made, but this still left Miss T at a considerable loss. She complained to Revolut who declined to provide further redress and the matter was referred to our service. One of our Investigators ultimately recommended that Revolut should pay Miss T around £9,630, that being her

outstanding loss, plus 8% interest. This took account of the fact that Miss T had received around £6,700 from N as a gesture of goodwill as a result of her complaint to them.

Miss T accepted this outcome, but Revolut didn't. They asked for an Ombudsman to review the complaint. In November 2024 I issued a provisional decision in which I said:

"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'm intending to reach a different outcome to that of our Investigator. So, I'm issuing this provisional decision to give both sides a further opportunity to comment before finalising my decision.

My first consideration is which (if any) of the payments in dispute were authorised by Miss T. Generally speaking Miss T will usually be liable for payments she's authorised and Revolut for payments that weren't authorised. The relevant regulations to this are the Payment Services Regulations 2017, (PSRs). The below table includes some of the key events / payments relevant to this complaint.

Payment Number	***Date / Time***	***Event***	***Notes***
	14 January 2023 6.46pm	*ApplePay added to new device.*	
1	*14 January 2023 7.00pm*	*£3,000 payment to 'B' (a cryptocurrency exchange)*	*Authenticated by Apple Pay*
2	*14 January 2023 7.04pm*	*£10,000 payment to 'A'*	*Authenticated by Apple Pay*
3	*14 January 2023 7.11pm*	*£50 payment to B*	*Authenticated by Apple Pay*
4	*14 January 2023 7.13pm*	*£300 payment to B*	*Authenticated by Apple Pay*
	14 January 2023 7.14pm.	*Declined £380 payment to B*	
5	*14 January 2023 7.24pm*	*£380 payment to B*	*Authenticated by Apple Pay*
6	*14 January 2023 7.47pm*	*£1,517.10 payment to 'T'*	*Card payment authenticated by 3DS*
7	*14 January 2023 7.51pm*	*£5,000 payment to 'U' **	*Authenticated by Apple Pay*
8	*14 January 2023 8.07pm*	*£433.64 payment to 'W'*	*Card Payment authenticated by 3DS*
9	*14 January 2023 8.14pm*	*£649.97 payment to T*	*Card payment authenticated by 3DS*
10	*14 January 2023 8.37pm*	*£750 payment to 'U' **	*Authenticated by Apple Pay*

*The payments marked with an * were returned to Miss T's account around a week later.*

I accept Revolut's technical evidence as to how each payment was authenticated (as set out in the table above). And I understand that Revolut's 3DS verification for a payment involves confirming it to be genuine from within Revolut's app.

Apple Pay being added to a device required the use of a code that was sent to Miss T's phone by Revolut. The message in full read "This code will be used to add your card to another Apple device. Don't enter it anywhere unless you want to add your card to a new device. Don't share this code with anyone, even if they claim to be from Revolut. Revolut verification code for Apple Pay: XXX-XXX"

Miss T's testimony about the sharing of this code and whether she authorised any payments hasn't been entirely consistent. During the chat with Revolut on 14 January 2023 the following exchange took place:

***Revolut:** "And you shared the a code that you received via SMS?"*
***Miss T:** "No"…*
***Revolut:** "The code that you received was shared with the person that called you, correct?*
***Miss T:** "No"*

Miss T also said "All transactions from 1900 onward were not made by me.. they are all fraudulent and not authorised by myself." Later in January 2023 Miss T also said: "But I never gave any pin and I don't remember that message ever coming through...I've never given anyone an otp or access to my Apple Pay so this is not a possibility without a shadow of a doubt."

But within the same chat Miss T also says the following: On 19 January 2023 "I do know for a fact that I did not confirm all of them maybe 2 or 3, not completely sure…" On 25 January 2023 "I know that on the day I did indeed authorise some of the transactions that took place but this was only for those of a much lower value…" And on 3 February 2023 "I never authorised the first three payments and in fact saw someone move money from inside my account to another (which would be the first three transactions) without me doing this on my app myself AND this was used to convince me they worked for Revolut by saying "see how I'm able to move money from inside your account without your prior authorisation that's because we have staff access to do so" which in turn convinced me to authorise the next one to three transactions but from memory this was no more than three at a push! And I'm sure this is the case as I would never have authorised the movement of such huge numbers from my account just like that." And finally in Miss T's letter of complaint with reference to the Apple Pay OTP she said: "Before reading the whole text message I was pressured into giving him the number quickly and being in the vulnerable, panicked, urgent and time-pressured situation I gave him the number."

Miss T having said different things at different times makes it difficult for me to place a lot of weight on her testimony as being credible and reliable evidence. The nature of a safe account scam is that money is moved on the premise that it is at risk where it currently is. So whilst Miss T says she wouldn't have agreed to payments of those values, she did when moving money from her account with N to her Revolut account. Miss T must have shared the OTP to allow Apple Pay to be added to a new device (indeed it now seems she accepts she did).

I've thought about this point carefully. Miss T says that she didn't approve all of the payments and it's clear that the first few payments required no additional verification – they were just processed using Apple Pay which the fraudsters had added to their device.

So, I accept that Miss T didn't actually instruct some of the payments herself – that was the fraudsters. But for me to conclude that Miss T authorised the payments, I only need to be satisfied that she gave her permission for someone to make payments on her behalf.

Miss T's testimony hasn't been entirely consistent but she does say that after she moved her money from N to her Revolut account she was told that her Revolut account had been

infected by malware and that her funds would need to be moved on again, to a new safe account. According to that testimony, she was told this prior to handing over the code which allowed Apple Pay to be set up on a new device and, therefore, before the fraudsters were able to 'demonstrate access to her accounts' by making the initial Apple Pay transactions.

There's no suggestion that Miss T didn't agree that her money should be moved from her Revolut account to the new safe account and her later action in approving payments demonstrate that she, at least at that point, agreed this was necessary. As I've set out, she's also given conflicting testimony about exactly what happened, which makes it difficult to put significant weight on her testimony.

All things considered, I think that Miss T, while not necessarily keying all the payments herself, agreed that money should be moved from her Revolut account to a new safe account prior to any payments being made, and therefore the payments should be considered as authorised. This is further supported by the fact that Revolut declined a payment and blocked Miss T's card between payments four and five. And that she then went into the app to say she recognised the payment and unblocked her card facilitating the further payments that followed.

But this isn't the end of the story and only relates to the application of the PSRs. Revolut should still fairly and reasonably be alert to the possibility of fraud, scams and the misappropriation of funds.

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the PSRs and the terms and conditions of the customer's account. And, as the Supreme Court has recently reiterated in Philipp v Barclays Bank UK PLC, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

- *The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.*
- *At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In Philipp, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a legal duty to do so.*

In this case, the terms of Revolut's contract with Miss T modified the starting position described in Philipp, by – among other things – expressly requiring Revolut to refuse or delay a payment "if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks" (section 20).

So Revolut was required by the terms of its contract to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I am satisfied that paying due regard to the interests of its customers and treating them fairly meant Revolut should

have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks.

In practice Revolut did in some instances refuse or delay payments at the time where it suspected its customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

Whilst the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in January 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMI's like Revolut did in fact seek to take those steps, often by:

- *using algorithms to identify transactions presenting an increased risk of fraud;*[1]
- *requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;*
- *using the confirmation of payee system for authorised push payments;*
- *providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.*

For example, it is my understanding that in January 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I am also mindful that:

- *Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and*

[1] For example, Revolut's website explains it launched an automated anti-fraud system in August 2018:
https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks_/

control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3)[2].

- *Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the "Financial crime: a guide for firms".*

- *Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.*

- *The October 2017, BSI Code[3], which a number of banks and trade associations were involved in the development of, recommended firms 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. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).*

- *Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.*

- *The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So it was*

---

[2] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

[3] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in January 2023 that Revolut should:

- *have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;*
- *have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;*
- *in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and*
- *have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.*

<u>Should Revolut have recognised that Miss T was at risk of financial harm from fraud?</u>

Payment one was to a cryptocurrency exchange. And I think Revolut likely would have been able to identify this at the time of the payment. I'm aware that cryptocurrency exchanges like B generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too.

So, it could have reasonably assumed that payment 1 would be credited to a cryptocurrency wallet held in Miss T's name. By January 2023, when this transaction took place, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time.

Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions. And by January 2023, when this payment took place, further restrictions were in place.

This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry. I recognise that, as a result of the actions of other payment service providers, many

customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut.

And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above I am satisfied that prior to the payments Miss T made in January 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

In practical terms, Revolut already does take some additional steps to further authenticate certain card payments. Examples of this are payments six, eight and nine which required Miss T to go into the Revolut app and take additional steps to confirm the payment. And in January 2023, with Miss T's payment (one) of the value of £3,000 which was identifiably going to a cryptocurrency exchange, I think Revolut ought to have identified that this payment presented a potential risk to her. Miss T's account had been open since 2021 and before payment one was instructed, the largest payment to have left the account was for only £150. The account was infrequently used and with very few outgoing payments, and none for any significant sums. Payment one also seems to be the first time Miss T had purchased cryptocurrency. These factors combined mean it was a departure from how the account had been used previously. And I think Revolut should have had some concern that Miss T might be at risk of financial harm.

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to Revolut's duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made. Taking that into account, I think Revolut ought, when Miss T attempted to make payment one, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam, without significantly losing impact. So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value. I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Miss T by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

However, I'm not persuaded that I can fairly say that displaying such a warning would have prevented this payment being made or have resulted in discovery of the scam. I can understand that Miss T might argue that she believed money was being moved to a safe

account and so knowing it was really being used to purchase cryptocurrency would have alerted her to what was going on. But payment eight is one example where Miss T did complete further authentication through the app (3DS) and that payment appeared to be going to a travel company, something Miss T would have seen. And as this didn't make a difference at the time, I don't think a warning about cryptocurrency scams would have either. I also note that Revolut did block Miss T's card after payment four and required her to reactivate it to continue making payments – something she followed the in-app guidance to do. The weight of the evidence suggests that Miss T, at that point in time, was following the scammers directions and not really taking in the information being presented to her if she could click through it to continue.

Payment two was instructed only a few minutes after payment one and wasn't to a cryptocurrency exchange. However the combination of the two payments meant spending of £13,000 in four minutes with £3,000 of that being to a cryptocurrency exchange. Both payments were instructed via ApplePay on a device that had been added to the account around 15 minutes earlier. The payments also followed soon after the arrival of around £13,000 from Miss T's account with N. This was an even more significant departure from how the account had been used previously. Taking all of this together I think Revolut ought to have identified the heightened risk associated with payment two.

Having thought carefully about the risk payment two presented, I think a proportionate response to that risk would be for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to be authorised. I think this should have been done by, for example, directing Miss T to its in-app chat to discuss the payment further.

<u>If Revolut had attempted to establish the circumstances surrounding payment two, would the scam have come to light and Miss T's loss been prevented?</u>

Had Miss T told the genuine Revolut that she was being asked to move money to a new account in order to protect those funds, they would have immediately recognised that she was falling victim to a scam. They would have been able to provide a very clear warning and, given that Miss T had no desire to lose her money and nothing to gain from going ahead with the payments, it's very likely that she would have stopped, not followed the scammer's instructions and her further loss would have been prevented.

So, I've considered whether Miss T would have revealed that she was being asked to move money to a safe account. Miss T hasn't said she was given a cover story, but I also accept that because there was no detailed scrutiny of the payments by Revolut, this may not have been required. As I've mentioned above, the evidence does suggest that Miss T was clicking through within the app as directed by the scammer. And I understand that these types of scam work in part due to creating a sense of urgency and panic against the threat of funds being lost. But in a chat (as opposed to in app warnings or notifications) there is less opportunity to quickly rush through. I know that in similar circumstances Revolut sometimes ask their customer to provide a selfie picture of themselves alongside a piece of paper displaying the payment purpose. This further helps to create a natural pause. I think such factors are important in thinking about what most likely would have happened. Miss T may have been rushed through things within the app by the scammer, but at all times this was because she thought she was being helped to protect her funds. And if the scammer had told Miss T to lie or otherwise hide the true purpose of her payments, I think this would have been a red flag to her.

Ultimately, as Revolut didn't question payment two, it can provide no compelling evidence to support that Miss T would have misled them about the purpose of her payment or the

surrounding circumstances. And the information from Miss T's complaint about N indicates that there weren't any interventions in the payments between them and the Revolut account.

So, Revolut should have, once they had established why Miss T was making the payment, provided a very clear warning that explained, as a minimum, that they would never ask her to move money to a new account, that phone numbers could be spoofed and that she was falling victim to a scam.

I think, on the balance of probabilities, that's likely to have caused Miss T to stop. She didn't want to lose her money and I can see no reason for her to have continued to make the payment if she was presented with a warning of this nature.

I think it's most likely that had Revolut established the circumstances surrounding payment two, as I think they ought to have done, and provided a clear warning, Miss T's loss from and including payment two would have been prevented.

Is it fair and reasonable for Revolut to be held responsible for Miss T's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Revolut were one of two firms involved here. Some of the funds sent on from Revolut were first received from Miss T's bank N.

But as I've set out in some detail above, I think that Revolut still should have recognised that Miss T might have been at risk of financial harm from fraud when she made payment two, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Miss T suffered. The fact that the money used to fund the scam came from elsewhere does not alter that fact and I think Revolut can fairly be held responsible for Miss T's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that our service currently only has an open complaint from Miss T against Revolut. Miss T did complain to N and referred the matter to our service. That complaint was resolved when she accepted just over £6,700 from N (something N offered without any admission of fault or liability). I accept that it's possible that N might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way. But I can't consider a complaint that has already been resolved by agreement between the parties. In these circumstances, Miss T is entitled to try to recover her outstanding loss from Revolut and in this decision, I can only make an award against Revolut.

Ultimately, I must consider the complaint that has been referred to me and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Miss T's loss from payment two.

Should Miss T bear any responsibility for her loss?

In considering this point, I've taken into account what the law says about contributory negligence as well as what I consider to be fair and reasonable in the circumstances of this complaint.

Having considered the matter carefully, I don't think that there should be any deduction from the amount reimbursed.

The tactics employed by the fraudsters are common, but nonetheless captivating to anyone unfamiliar with them.

Miss T says she was previously unaware that numbers could be spoofed and when she checked at the time, she thought the caller's number was genuinely associated with Revolut. It was only later that she established there was one digit that was different to the genuine number, something Miss T puts down to her dyslexia. While Revolut may argue that had Miss T more accurately checked the number, she would have identified the discrepancy. I can also see that Miss T spent more than two hours on the phone to the fraudsters. And I don't think that this gave her the chance to reflect on what she was being told.

Miss T did also unblock her card which allowed payments to continue as well as completing further authentication for payments that didn't fit in with what she believed at the time. As I've mentioned above, the card payments seemed to go to companies rather than to a new account in Miss T's name. It is easier in hindsight to highlight these factors. But I have to think about the situation as it was at the time. Miss T said the scammer maintained the sense of urgency and pressure – "They made me feel anxious, vulnerable and worried about the situation but made me feel reassured and convinced me that they were there to help".

It is common knowledge that these types of scams do rely on fear and urgency to help gain compliance before the victim has a chance to step back, think and potentially realise what is happening. Overall, I don't think there should be a deduction to the amount reimbursed. Miss T clearly didn't want to lose her money. Her actions cannot be explained by carelessness or personal gain. There's little other explanation than that she believed what she was told by some very sophisticated fraudsters and in the circumstances, I don't find her belief to be unreasonable.

Some of Miss T's submissions refer to her being vulnerable. This isn't something I can see Revolut were informed of prior to any of her payments. So I don't think there was anything I'd have expected Revolut to have done differently based solely on her vulnerability.

What should be done to put things right?

Miss T paid a total of £22,080.71 from her account. £5,750 of this (payments seven and ten) were recovered. Miss T also received £6,700.23 from N (as a gesture of goodwill) to resolve her complaint with them. This leaves her outstanding loss (that which Revolut could potentially be found responsible for) as £9,630.48. Any sum greater than this would put Miss T in a better position, which would clearly be unfair. And for the reasons I've covered above, I don't think Revolut are responsible for the initial payment of £3,000.

As a result of this, in the circumstances of this complaint, I think it would only be fair and reasonable to ask Revolut to pay £6,630.48. This is the total amount sent less the sums I've listed above.

I also think that as Miss T was without the funds she otherwise would have had, that 8% simple interest should be added in the following way. Between the date of loss and the date that N paid Miss T the £6,700.23 Revolut should pay the interest on the amount of £13,330.71. This is because the money N paid, could've been prevented from leaving Miss T's Revolut account and no interest was included in their settlement offer. And from the date that money was received until the date of settlement, the same 8% simple interest should be paid on the amount of £6,630.48.

My provisional decision

For the reasons outlined above, but subject to any further information I receive from either Revolut or Miss T, I intend to uphold this complaint.

I intend to direct Revolut Ltd to pay Miss T £6,630.48.

8% simple interest should also be paid in the following way. Between the date of loss and the date Miss T received the £6,700.23 from NatWest it should be paid on the sum of £13,330.71. And from that date onwards, until the date of settlement, it should be paid on £6,630.48."

Revolut didn't respond to my provisional decision. Miss T responded to say she accepted it.

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.

As neither party had any further comments or evidence for my consideration, I see no reason to deviate from the outcome explained in my provisional decision.

My final decision

For the reasons outlined above, my final decision is that I uphold this complaint.

Revolut Ltd must pay Miss T £6,630.48.

8% simple interest should also be paid in the following way. Between the date of loss and the date Miss T received the £6,700.23 from NatWest, it should be paid on the sum of £13,330.71. And from that date onwards, until the date of settlement, it should be paid on £6,630.48.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss T to accept or reject my decision before 19 December 2024.

Richard Annandale
Ombudsman