

The complaint

Mr H is unhappy that Revolut Ltd (“Revolut”) didn’t reimburse him after he fell victim to a scam.

What happened

The background to this complaint is well-known to both parties, so I won’t repeat it in detail here, but in summary, I understand it to be as follows.

In or around March 2023, Mr H saw an advertisement on a social media platform promoting an investment opportunity. It appeared to have been endorsed by a well-known public figure. He followed a link on the advert and completed a form to register his interest with the company purporting to promote it. Unfortunately, this wasn’t a genuine investment opportunity, but a scam.

Someone called him who claimed to be an employee of the company and Mr H was then put in contact with somebody claiming to be a financial advisor. He told Mr H that he would show him how things work and help him set things up. Mr H was given access to a trading platform, which appeared to show how his investment was performing. The fraudster told Mr H that he’d be able to realise a profit of at least 33%.

Believing everything to be genuine Mr H made an initial payment, from an account he held with another financial firm. He could see the credit on the trading platform and over the coming days was able to see profits rising and was able to make a withdrawal (for £100) which reassured him further.

Mr H was then instructed by the fraudster to set up a Revolut account in order to facilitate further payments. He was instructed to purchase cryptocurrency from a number of cryptocurrency exchange platforms (with whom he’d set up accounts). Once his money had been converted into cryptocurrency it was then sent to accounts controlled by the fraudsters.

Mr H made an initial payment from his Revolut account of £900. The fraudsters told him that the more he invested, the higher the returns and that he should invest a least £5,000. Mr H has said he was adamant he didn’t want to invest more and asked to withdraw his funds.

Following this Mr H was told that a further payment needed to be made in order to withdraw his money, which Mr H thought was commission for the services he’d been provided. He was then told more money was needed, due to regulations. Mr H has said he felt pressured to make the payments, as he was worried that if he didn’t pay he would lose all that he’d invested. He was also told by the fraudsters that in order to withdraw any money, he would need to download remote access software.

Thinking he needed to make payments in order to gain access to his money, Mr H made the following transactions from his Revolut account;

7 April 2023	£900	card payment to cryptocurrency account 1
29 June 2023	£2,000	card payment to cryptocurrency account 2

30 June 2023	£3,500	card payment to cryptocurrency account 2
1 July 2023	£3,500	card payment to cryptocurrency account 2
4 July 2023	£3,200	card payment to cryptocurrency account 2

Mr H realised he'd been scammed when the fraudsters cut contact with him and he was unable to reach them. He raised the matter with Revolut, but it didn't think it was liable for the loss Mr H had suffered. In summary it said all correct procedures were followed and it also didn't think it had any rights to raise a dispute through the Chargeback scheme.

Unhappy with Revolut's response, Mr H brought the matter to this service. One of our Investigator's looked into things and thought the complaint should be upheld in part. In summary, our Investigator thought Revolut ought to have warned Mr H at the point he was making the third payment (the payment for £3,500 on 30 June 2023 in the table above). Had it done so, it was our Investigator's view that Mr H wouldn't have proceeded with this, or the subsequent payments.

But our Investigator also thought Mr H should bear some responsibility for his loss. In summary, our Investigator thought the returns Mr H was initially promised, of 33%, were unrealistic and the rate of returns he was seeing were implausible. Overall, our Investigator recommended that Revolut refund Mr H 50% of his loss from the final three payments he made to the fraudster, along with interest.

Mr H accepted our Investigators view. But Revolut disagreed, in summary it set out the following points:

- This service is permitted to depart from the law, but where we do, we should explain that we have done so and explain why. If we apply the law or legal duties, we should apply it correctly and if we err in law, we are susceptible to judicial review on the grounds of error in law in relation to our identification of what the law is (as well as perversity and irrationality).
- Revolut is bound by contract, applicable regulations and common law to execute valid payment instructions. The duty is strict and there are only limited exceptions.
- Revolut referred to specific terms in its terms and conditions and went on to say that although the relationship between a payment service provider (like Revolut) and a customer is one of contract, such contracts are performed in a heavily regulated legal environment. The most significant legislation is the Payment Services Regulations 2017 which impose obligations to execute authorised payments promptly. By suggesting that it needs to reimburse customers, it says our service is erring in law.
- This service has overstated Revolut's duty. Revolut recognises its obligations and has put adequate procedures in place. But the duty is not absolute and doesn't require Revolut to detect and prevent all fraud.
- It does not need to concern itself with the wisdom or potential for financial loss of a customer's payment instructions. This was confirmed in the recent Supreme Court judgement in the case of Philipp v Barclays Bank UK plc [2023] UKSC 25.
- Our service appears to be treating Revolut as if it were a signatory to the Contingent Reimbursement Model Code.
- The payments in question are in reality self-to-self payments. The fraudulent activity did not occur on the customer's Revolut account, as the payments being made were to perform legitimate cryptocurrency purchases to accounts held in the customer's own name.

As agreement couldn't be reached, the complaint has been passed to me for a final decision.

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.

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 Payment Services Regulations (in this case the 2017 regulations) 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 Mr H 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 April 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 April 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 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

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/

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.

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 Code³, 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 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 that during the period of these payments, between April 2023-July 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

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

- 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.

Whilst I am required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I am satisfied that to comply with the regulatory requirements that were in place during the period of these payments, between April 2023-July 2023, Revolut should in any event have taken these steps.

Should Revolut have recognised that Mr H was at risk of financial harm from fraud?

It isn't in dispute that Mr H has fallen victim to a cruel scam here, nor that he authorised the payments he made by debit card to his crypto wallets (from where that crypto was subsequently transferred to the scammer).

Whilst I have set out the circumstances which led Mr H to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr H might be the victim of a scam.

I'm aware that crypto exchanges, like the ones Mr H made his payments to here, generally stipulate that the card used to purchase crypto 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 the payments would be credited to a crypto wallet held in Mr H's name.

By April 2023, when these transactions started, firms like Revolut had been aware of the risk of multi-stage scams involving crypto for some time. Scams involving crypto have increased over time. The FCA and Action Fraud published warnings about crypto scams in mid-2018 and figures published by the latter show that losses suffered to crypto scams have continued to increase since. They reached record levels in 2022. During that time, crypto 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 crypto using their bank accounts or increase friction in relation to crypto related payments, owing to the elevated risk associated with such transactions. And by April 2023, when these payments began, 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 crypto 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 PSPs, many customers who wish to purchase crypto 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 crypto 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 crypto provider, a fact that Revolut is aware of.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr H made from April 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 crypto, notwithstanding that the payment would often be made to a crypto wallet in the consumer's own name.

To be clear, I'm not suggesting that, as a general principle, Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with crypto in April 2023 that, in some circumstances, should have caused Revolut to consider transactions to crypto providers as carrying an increased risk of fraud and the associated harm. In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before they processed such payments. And as I have explained Revolut was also required by the terms of their contract to refuse or delay payments where regulatory requirements meant they needed to carry out further checks.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving crypto, I don't think the fact payments in this case were going to an account held in Mr H's own name should have led Revolut to believe there wasn't a risk of fraud. So, I've gone on to consider, taking into account what Revolut knew about the payments, at what point, if any, they ought to have identified that Mr H might be at a heightened risk of fraud that merited its intervention.

I'm satisfied that there was nothing about the first two payments that ought to have looked concerning to Revolut. Though they were identifiably being made to cryptocurrency platforms, this matched the purpose that Mr H had given for opening his account (Crypto and Transfer) and I don't think the value of the payments, in and of themselves, ought to have given Revolut cause for concern. And so, I don't think there would've been enough reason for Revolut to suspect that they might have been made in relation to a scam.

However, by the time the third payment was made, I think there was enough going on that ought to have given Revolut some cause for concern. This was the second payment to a new payee (which was identifiably being made to a cryptocurrency platform) within a short period of time, with the value increasing between each payment and meaning, cumulatively, Mr H was sending over £5,000 within the space of a day.

What did Revolut do to warn Mr H?

From what I've seen there isn't any evidence to show that any warnings were provided by Revolut. But rather, the only steps taken were part of the 3DS authentication process.

What kind of warning should Revolut have provided?

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 Mr H attempted to make the payment on 30 June 2023, knowing (or strongly suspecting) that the payment was going to a crypto provider, to have provided a tailored warning that was specifically about the risk of crypto 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 crypto 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 crypto scams – crypto 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 crypto investment scams, for example referring to: an ‘account manager’, ‘broker’ or ‘trader’ acting on their behalf; moving crypto to a third-party trading platform; the use of remote access software; the promise of large returns for seemingly little or no risk; the prevalence of these scams being advertised through social media platforms; endorsements by well-known public figures or celebrities and a small initial deposit which quickly increases in value.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr H suffered from the third payment?

I’ve carefully considered what I think would have most likely have happened, had Revolut provided a warning as I’ve described above. On balance, I’m persuaded that a specific warning covering off the key features of crypto investment scams would’ve prevented Mr H from proceeding with the payment for £3,500 (made on 30 June 2023) – and he wouldn’t have lost the money from this, or the subsequent payments.

I say that as there were several key hallmarks of common cryptocurrency investment scams present in the circumstances of the payment Mr H was intending to make. Including, but not limited to, the promise of high returns, a celebrity endorsement through a social media channel, being asked to download remote access software, being in contact with a broker and being asked to move funds through trading platforms. I think it’s more likely than not that seeing how these scams typically play out would have echoed with what he was experiencing and the similarities, I’m persuaded, would have prevented him from proceeding any further.

I’m also mindful, in the individual circumstances of this case, there is no evidence to suggest that Mr H was asked, or agreed to, disregard a warning provided by Revolut. And I note that I’ve also seen no evidence that Mr H was provided with warnings by the firm from which the funds used for the scam appear to have originated.

Revolut has argued that we are applying the provisions of the CRM Code to complaints against it, despite it not being a signatory. I have no intention of treating Revolut as if it were a signatory to the CRM Code. I’ve explained in some detail the basis on which I think, fairly and reasonably, Revolut ought to have identified that Mr H was likely at risk of financial harm from fraud, and the steps it should have taken before allowing the payments to debit his account.

Overall, on the balance of probabilities, had Revolut provided Mr H with an impactful warning that gave details about crypto investment scams and how he could protect himself from the risk of fraud, I believe it would have resonated with him and he wouldn’t have gone on to make this or the subsequent payments.

Is it fair and reasonable for Revolut to be held responsible for Mr H’s loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mr H purchased cryptocurrency which credited e-wallets held in his own name, rather than making a payment directly to the fraudsters. So, he remained in control of his money after he made the payments from his Revolut account, and it took further steps before the money was lost to the fraudsters.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr H might have been at risk of financial harm from fraud when he was making the third transaction, 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 Mr H suffered.

The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to Mr H's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr H'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 Mr H has only complained against Revolut. I accept that it's possible that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Mr H could instead, or in addition, have sought to complain against those firms. But Mr H has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr H's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be 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 Mr H's loss from the third transaction, subject to a deduction for his own contribution which I will consider below.

Should Mr H bear any responsibility for their losses?

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

Mr H has already accepted the Investigator's opinion that any refund provided should be reduced to account for his own actions as part of the scam and as I agree with this point, I won't dwell on it, except to say that I think there were a number of things that ought to have led Mr H to proceed with more caution than he did.

I recognise that there were some relatively sophisticated aspects to this scam, not least a platform, which was used to access and manage the user's apparent profits/trades and I can understand how Mr H would have been reassured by receiving some funds back into his account.

From what Mr H has told us, he doesn't seem to have done any other independent checks of his own. Alongside this Mr H has said that he wasn't provided, nor did he ask for, any documentation, such as a contract – setting out the terms of any investment arrangement between the two parties.

As well as this, Mr H has said that he was told that he could expect to receive a minimum profit of 33%. It seems more likely than not to me, that this level of return, with seemingly little or no risk, was implausible to the point of being too good to be true. But I can't see that

Mr H questioned how such high levels of returns could be realised, rather he seems to have taken things at face value.

I think the payments Mr H was asked to make by the fraudsters ought also to have given him some concern. While I might understand why Mr H would think he may have to pay some commission, I think it's questionable why he would have had to make ancillary payments, for in excess of £12,000, for an investment of just £900.

I'm also mindful, in the individual circumstances of this case, there were some negative reviews online about the company Mr H thought he was investing in and there was a warning about the company on the Financial Conduct Authority (FCA's) register. So I'm persuaded it wouldn't have taken much, by way of research, to have established that things might not be as they first seemed.

I might understand how in isolation any one of these things may not have prevented Mr H from proceeding. But when taken collectively I think, there were sufficient red flags here that reasonably ought to have led Mr H to have acted far more cautiously than he did.

Could Revolut have done anything to recover Mr H's money?

The payments were made by card to legitimate cryptocurrency exchanges. Mr H sent that cryptocurrency to the fraudsters. So, Revolut would not have been able to recover the funds. In addition, I don't consider that a chargeback would have had any prospect of success, given there's no dispute that the cryptocurrency exchange provided cryptocurrency to Mr H, which he subsequently sent to the fraudsters.

Putting things right

For the reasons explained, I uphold this complaint in part and now ask Revolut Ltd to:

- refund Mr H £5,100 (being 50% of the sum of the final three payments).
- pay interest on this amount calculated at 8% simple per year from the date of loss to the date of settlement (if Revolut Ltd deducts tax from this interest, it should provide Mr H with the appropriate tax deduction certificate).

My final decision

For the reasons given above my final decision is that I uphold this complaint in part.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 4 April 2025.

Stephen Wise
Ombudsman