DRN-5388357

The complaint

Mrs A complains that HiFX Europe Limited trading as Xe ("Xe, hereinafter") won't refund the money she lost after she fell victim to an investment scam.

What happened

The facts are well known to both parties, so I have outlined the key details. In summary, Mrs A and her mother were approached out of the blue by a lawyer based in the US, who claimed to have found Mrs A's mother's lost shares from a previous investment made many years before.

The lawyer explained Mrs A's mother could realise the value of these shares by selling them back to the company they originated from, if she paid the fees necessary to do so. Mrs A said she carried out checks on the lawyer to ensure this was a legitimate contact. However, this was sadly a scam.

Mrs A's mother was 77 years old at the time the scam took place, so Mrs A offered to assist her by using her own banking and payment facilities. Most of the funds used towards the scam stemmed from an inheritance of Mrs A's mother. Mrs A also used some of her funds towards the payments, on the understanding that some of the profits from the sale of the shares would go to her.

Mrs A used her accounts with a bank I'll refer to as N, to receive her mother's and her own funds in. From there, she made payments to the scammer using Xe. Some of the payments, before landing into Mrs A's account with Xe, went through her account with an electronic money provider I'll refer to as R.

From her Xe account Mrs A made the following payments (the credits into the account are highlighted in bold):

Payment #	Date	Time	Type of transaction	Amount
	8 November 2023		**Debit card top up from Mrs A's account with N**	**+£19,297.79**
1	8 November 2023	16:21	International payment to scammer's account	$23,634.00
	21 November 2023		**Debit card top up from Mrs A's account with N**	**+£18,888.02**
2	21 November 2023	01:24	International payment to scammer's account	$23,543.92
	22 November 2023		**Debit card top up from Mrs A's account with N**	**+£18,851.73**
3	22 November 2023	00:36	International payment to scammer's account	$23,543.92
	6 December 2023		**Debit card top up from Mrs**	**+£4,959.64**

			A's account with N	
	6 December 2023		**Debit card top up from Mrs A's account with N**	**+£25,000.00**
4	6 December 2023	13:29	International payment to scammer's account	$31,190.00
5	6 December 2023	16:15	International payment to scammer's account	$6,223.85
	12 January 2024		**Faster payment from Mrs A's account with R**	**+£12,643.30**
6	12 January 2024	12:34	International payment to scammer's account	$16,140.30
	5 February 2024		**Debit card top up from Mrs A's account with N**	**+£19,236.93**
7	5 February 2024	20:13	International payment to scammer's account	$24,000.00
TOTAL				**$148,275.99**

Mrs A realised that she had fallen victim to a scam after months of payments and delays, which prompted her to take a trip to the US and visit the scammer's offices in person. She then found out there were no offices at the address she had been given and all contact with the scammer ceased.

Mrs A raised scam claims with N, R and Xe. Xe stated that, as Mrs A had just opened the account, it didn't have sufficient transactional data to determine whether the transactions were suspicious. Xe added that Mrs A had selected the wrong payment reason, resulting in Xe not becoming alert to the possibility she may be scammed. Xe refused to refund Mrs A for any of the scam payments. It said that, due to the nature of the services Xe offered, Mrs A's bank N would have been in a better position to detect any anomalies and issue her with a refund.

So, Mrs A referred the complaint to the Financial Ombudsman Service.

In the linked complaint against N, our Investigator found that N should refund 33% of the payments made directly to Xe and 50% of the payments Mrs A made to her account with R, and that Mrs A should be held equally liable for her loss. Both N and Mrs A have accepted that outcome and N has already refunded Mrs A in the way the Investigator recommended.

In this complaint, our Investigator found that all payments, starting from the first one, were high value and unusual enough that Xe should have blocked them and queried them further with Mrs A. Our Investigator said they had found no evidence of coaching from the scammer and that, therefore, a good intervention would have unveiled the scam.

However, in line with their findings on the linked complaint, Mrs A should also be responsible in equal measure to the firms involved. So, they recommended Xe refunded 17% of the funds lost to the scam, which, together with the refund Mrs A had received from N (33%), would mean she would be responsible for the remaining 50% of her loss.

Xe disagreed with our Investigator's view, stating that Mrs A had breached the terms and conditions of her agreement with Xe when she made payments through its facilities on behalf of a third party (her mother). So, it would not be fair to hold Xe liable in the circumstances.

Moreover, it said the nature of the services Xe offers means that customers usually make larger one-off payments through its platform, so it can't be asked to scrutinise payments

exclusively on the basis of their amount, as that would effectively result in it having to block them all. Xe maintained its position that there wasn't sufficient information around the payments to determine Mrs A was at risk of being scammed and so it should not be asked to refund her.

In light of this disagreement, I have been asked to review everything afresh and reach a decision on the matter.

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.

I'm aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focused on what I think is the heart of the matter here. 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 point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

Where the evidence is incomplete, inconclusive, or contradictory, I must make my decision on the balance of probabilities – that is, what I consider is more likely than not to have happened in the light of the available evidence and the wider surrounding circumstances. I've thought carefully about whether Xe treated Mrs A fairly and reasonably in its dealings with her, when she made the payments and when she reported the scam, or whether it should have done more than it did.

Having done so, I agree with the conclusions reached by our Investigator, and broadly for the same reasons. I consider Xe should, at the least, have blocked and queried the first payment Mrs A made to the scammer from its payment facilities. If it had done so, I'm satisfied the scam and losses to Mrs A from that payment onwards, would more likely than not have been prevented. But I am also satisfied that in the circumstances of this complaint, Mrs A should bear some responsibility (50%) for the losses she suffered.

I have kept in mind that Mrs A made the payments herself, and the starting position is that Xe should follow its customer's instructions. So, under the Payment Services Regulations 2017 (PSR 2017) she is presumed liable for the loss in the first instance.

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.

So, considering the relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time – Xe should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and 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 payment service providers are generally more familiar with than the average customer.

- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases decline to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.
- Have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so.

Should Xe have intervened?

So, I've thought about whether the scam payments should have highlighted to Xe that Mrs A might be at a heightened risk of financial harm due to fraud or a scam.

The evidence before me shows that Xe didn't intervene at all during any of the payments Mrs A has made. Xe shared with our service a copy of its payment review page, showing a link to "tips for sending money". As that "tips for sending money" page wasn't part of the payment journey itself and wasn't generated in response to the risks identified in the transaction Mrs A was making, I don't think it qualifies as a fraud warning or intervention on the payment.

I'm mindful that Xe didn't have historic information about the account or what Mrs A's typical usage was like, because she had just opened her account with Xe when she made the first payment. So, Xe wouldn't have been at first in a position to know whether Mrs A's activity was unusual or out of character – as it had nothing to compare it against.

However, I've found that Xe should have still blocked and intervened on the first payment Mrs A attempted from its payment facilities on 8 November 2023, due to the value of the payment, which was high enough in itself to warrant further questioning and probing of Mrs A's reasons for making it.

I have carefully considered Xe's argument that its facilities are regularly used by its customers to make high value payments, but that reason can't justify its lack of intervention, when the size of those payments could cause its customers severe financial harm, were they to be sent to a scammer.

I think that, precisely because Xe's customers are used to making larger than usual payments, Xe should have mechanisms in place to detect whether its customers may be at risk of being scammed before the payment is made.

Xe said that it asked Mrs A to select the payment reason, and she chose she was paying a bill. Xe argued it couldn't have realised Mrs A was at risk of suffering from financial harm because she hadn't selected she was making an investment, but I disagree that Mrs A made a misleading selection, and I disagree that her answer should have given Xe reasonable ground to classify the payment as safe.

I say this because Mrs A didn't think she was making a fresh investment but rather paying fees and taxes to release an earlier investment that her mother had made. So, I think her selection was coherent with what she thought she was paying for.

I would expect Xe to be aware by now of the prevalence of advance fee scams and invoice interception scams, where the victims are often expected to pay a bill. So, I don't think that Mrs A's selection of that option should have given Xe any reassurances as to the legitimacy of the payment.

I think the sheer size of the payment should have prompted Xe to ask a number of open-ended questions to ascertain what bill Mrs A was paying for and ask to see any invoices and documentation linked to that invoice. Had Xe ran a very basic check on the payee details online, it would have become immediately apparent that the funds were going to a company that had been dissolves since 2016.

I believe that, if Xe had probed Mrs A appropriately as to what she knew about the payee and the law firm that had approached her out of the blue, this would have prompted Mrs A to reconsider the premises of the scam and question whether these requests for payment were genuine. I'm also confident Xe would have been able to easily find out that the law firm was a scam, had it researched it online.

Our service hasn't seen any evidence of Mrs A being coached to lie to her banks by the scammer, and I don't think her payment purpose selections were the consequence of Mr A actively trying to mislead Xe as to the genuine reasons for her payments. Mrs A believed that she had been approached by a real lawyer and thought she was going through these payments to ensure she could withdraw the proceeds of this sale.

I'm persuaded that Mrs A thought this was a legitimate opportunity and so I believe she would have most likely co-operated with Xe's and responded truthfully to its questions, as she would not have had any reasons to lie.

Ultimately Mrs A uncovered the scam by herself, by travelling to the US to meet the scammer in person, which further supports my assertion that Mrs A was determined to find the truth and that the scammer's spell wasn't unbreakable. So, I think she would have welcomed Xe's input and scrutiny of her transactions.

In light of the above findings, I believe that, more likely than not, proportionate questioning from Xe would have unveiled the scam and prevented all of Mrs A's losses.

Xe has argued that it shouldn't be asked to refund Mrs A after she broke its terms and conditions by acting for her mother. However, I don't think that a breach of this nature negates Xe's responsibilities to protects its customers from foreseeable harm, as I've set out in quite some detail, above.

Moreover, I'm not fully persuaded that Xe has proven Mrs A breached its terms and conditions either, as she contributed some of her funds towards the scam and was expected to receive part of the proceeds from the sale of the shares. So, I think that, whilst it was convenient for her to make the transactions from her account to assist her mother, Mrs A was looking out for her own interests and making the payments in her own name too.

For the reasons I've set out above, I'm satisfied that around the time Mr A was making these payments Xe should have recognised that its customer could be at increased risk of fraud when using its services to make international payments and, therefore, it should have taken appropriate measures to counter that risk to help protect her from financial harm from fraud.

Did Mrs A contribute to her own losses?

I've thought about whether Mrs A should bear any responsibility for her losses. In doing so, I've considered what the law says about contributory negligence, as well as what I consider

to be fair and reasonable in all of the circumstances of this complaint, including taking into account Mrs A's own actions and responsibility for the losses she has suffered.

I recognise that, as a laywoman who claims to have little investment experience, there were aspects to the scam that would have appeared convincing. Mrs A has recalled that the scammer and their law firm came across as very professional, with a legitimate looking website, and several counterfeited documents and forms that mimicked genuine legal processes.

However, the scam opportunity also presented itself with some very clear red flags from the outset, which I believe should have given Mrs A great cause for concern.

I say this because Mrs A's initial correspondence to the scammer on 16 July 2023 shows she thought her own mother had been scammed, when she purchased these shares back in 2005, with no contact having been received since.

So, I think it would have been reasonable for Mrs A to be very sceptical when this lawyer from the US contacted her out of the blue about the scam investment, almost 20 years after it happened. My understanding is that Mrs A attempted to verify the scammer's details by approaching someone else within the firm he had claimed to be working for.

Unfortunately, though, Mrs A didn't take any independent steps to conduct any such verification and relied on the links and information the scammer fed to her, which naturally weren't aimed at her unveiling the scam, but rather believing it.

In Mrs A's email chain of 16 July 2023 with the scam law firm, she explained her mother had been scammed when purchasing those shares in 2005. She also asked for guidance on how to ascertain this wasn't a scam. The scammer's reply didn't acknowledge what Mrs A had said and didn't give any guidance or reassurance to her about this not being a scam. It simply confirmed that the contact she had received was from someone in their mergers and acquisitions department.

I don't think a reasonable person in Mrs A's position would have deemed this reply to satisfy any possible concerns as to whether this may be a scam. However, Mrs A didn't question the reply she'd received or seek the opinion of someone with more experience than her or a professional third party and proceeded to take the scammer's advice and overall situation at face value.

From that same correspondence, it also transpires that Mrs A was worried and suspicious about the email she had received. Mrs A's email to the scam law firm show she correctly identified that the scammer providing her with the personal details of another client, who also sold shares through their service, didn't seem to be compliant with data protection regulations and, more generally, the actions of a professional lawyer. But instead of acting on her instincts, she let her suspicions be swept away by the scammer.

Mrs A told our service that she also researched the scammer's law firm online when the scammer first made contact with her, but she didn't find anything untoward about it. But I think it would have been reasonable to expect Mrs A to take steps beyond mere online research, especially in light of her mother's and her own lack of investment experience, the contact coming after her mother had been scammed, and the amounts of money the scam lawyer was demanding of them.

Through my own research I found a blog post on a renowned free legal advice platform in the UK. This was posted before Mrs A started to make payments to the scammer and involved a very similar scenario to Mrs A's situation, including the same address for the

scam law firm. I think this post would have been easily accessible for Mrs A and that it should have resonated with her.

The US government department that the scammer mentioned to justify further requests for payments had never existed. Sadly, the website was deactivated only after Mrs A had made the scam payments. However, I would have expected Mrs A to verify both the law firm and government department had a traceable and reliable presence online beyond their own websites, such as being referenced in other government/institutional websites, being cited in newspaper articles, having their own profiles and accounts on social media platforms, etc.

Moreover, the international business account Mrs A was asked to pay belonged to a limited company that had been dissolved in 2016. I think these were discoverable red flags that Mrs A, despite not being an expert, could have identified, had she carried out independent online research or sought the assistance of a professional third party, if she remained unsure.

Even if Mrs A hadn't come across any of the above, given the size of payments she was asked to make and her and her mother's inexperience with investments, I would have expected her to check online that the law firm the scammer claimed to be working for was regulated in the US and to have an independent and competent third party review the paperwork and communication she had received. Had this happened, the scam would have been easily unveiled.

Overall, looking at the circumstances, I think Mrs A should have, on the balance of probabilities, realised there was a possibility the situation was not genuine and acted accordingly, much earlier than she did. As such, it would not be fair to require Xe to compensate her for the full amount of her remaining losses. Weighing the fault that I've found on both sides, I've concluded, on balance, that a fair deduction would be for Mrs A to bear 50% of her losses.

Finally, Mrs A has also argued that both her and her mother were vulnerable due to two recent bereavements in the family at the time of being approached by the scammer. While I note Mrs A's comments and I extend my condolences for her losses, the evidence I've seen doesn't suggest that Xe had been notified of any vulnerabilities or needs such that it should have known to take additional steps to protect Mrs A at the time the scam payments were made.

Recovery

All of Mrs A's scam payments went to an international payee. Xe has shown it initiated recovery efforts shortly after 16 May 2024, when he was notified by N that Mrs A had been scammed. However, this was about three months after Mrs A had made the last payment to the scammer.

Given that scammers are known for moving funds out of the receiving account within minutes, or hours at most, and considering that the chances of recovering funds from an international beneficiary are incredibly slim, I believe that, no matter how prompt Xe's efforts, Mrs A's funds were unlikely to be recovered in the circumstances.

So, I don't think it would be fair and reasonable to conclude that Xe should have done anything more to try and recover Mrs A's funds.

Calculating the refund

When taking into account the outcomes of the other complaints linked to this one, I've realised our Investigator included in their calculation of the refund, the losses Mrs A suffered when using R to make the payments to Xe.

As I've mentioned above, N has already refunded 50% of the funds Mrs A lost when she made the payment to Xe on 12 January 2024, which she had sent via her account with N, and then her account with R.

Since I've said she should bear 50% of her losses, I don't think Mrs A is owed a further refund of that payment. So, the payment of 12 January 2024 should not be included in the calculations of the refund Xe should pay to her.

I've also explained that N has already agreed to and refunded 33% of Mrs A's losses for which Xe was the exiting account. It follows from the above that, Xe is only required to refund 17% of Mrs A's losses to make up the 50% refund of what Mrs A lost through the scam.

I will explain below what this means in practice.

Mrs A's gross loss amounts to $148,275.99. The payment of 12 January 2024 amounts to $16,140.30. So, Mrs A's net losses come to $132,135.69.

Xe's liability is apportioned as follows: 17% of $132,135.69, that is $22,463.07.

Putting things right

To put things right, HiFX Europe Limited trading as Xe should now:

- Pay Mrs A 17% of the payments she made from the first payment onwards (minus the payment of 12 January 2024) – a total of $22,463.07.
- Pay 8% simple interest per annum on $22,463.07 from the date of each payment to the date of settlement*

I consider that 8% simple interest per year fairly reflects the fact that Mrs A has been deprived of this money and that she might have used it in a variety of ways.

*If Xe considers that it's required by HM Revenue & Customs to deduct income tax from the interest I've awarded, it should tell Mrs A how much it's taken off. It should also give Mrs A a tax deduction certificate if she asks for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.

My final decision

For the reasons given above, I uphold this complaint in part and require HiFX Europe Limited trading as Xe to pay Mrs A as I have set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A to accept or reject my decision before 11 February 2026.

Daria Ermini
Ombudsman