DRN-3377588

The complaint

Mr M is complaining HiFX Europe Limited (referred to as "Xe") won't refund a transaction he didn't authorise.

What happened

- Mr M said he was called by someone who claimed to be from BT Broadband Security on 21 September 2021. He recalled they told him there were several international users using his broadband account and they would need to be removed for security reasons.

- Mr M remembered that he was sent a link to AnyDesk to resolve the security problem. He was told the screen would go blank and come back, which he noted happened on several occasions.

- That day, a transfer for €10,381.84 was made from his Xe account – paid for by transferring £8,965.32 from Mr M's account with another bank.

- Mr M's other bank agreed to refund 50% of the money transferred. Xe disagreed that it's liable for the other half. It said its terms and conditions don't suggest that Mr M gets his money back from unauthorised scams, where the payment was correctly authenticated. And that he failed to keep his security details safe.

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.

Having done so, I agree with the conclusions reached by the investigator for these reasons:

- In line with the Payment Services Regulations 2017 (PSRs), Mr M isn't liable for payments he didn't authorise, unless he failed with gross negligence or intent to comply with the terms of the account or keep his personalised security details safe.

- I've firstly considered whether Mr M authorised the payment. Xe highlighted regulation 75(1) of the PSRs, which broadly says that where Mr M has denied authorising a payment, it's for Xe to show it was correctly authenticated. Xe submitted that because it's done that, Mr M can't claim it wasn't authorised.

- But that contradicts regulation 75(3) of the PSRs. This broadly says that a payment's correct authentication isn't enough to show that a payment was authorised.

- Instead, to determine authorisation, I must consider regulation 67 of the PSRs. This says that a payment is to be regarded as authorised if Mr M consented to it – and that consent must have been given in the form, and in accordance with the procedure, agreed between Xe and Mr M.

- To understand what the form and procedure was, I've reviewed the account terms and conditions Xe has provided our service. Under regulation 14.6 *"Consent to carry out a payment"*, it says

> *You can place Requests for Payments in writing or via telephone or via any other method we make available to you. Your Request: (a) should include all the details we require (including relating to the Beneficiary Account) to perform a Payment; and (b) will be treated by us as your consent to us to go ahead with and our authorisation to execute that Payment."*

- *"You"* is defined "you, our customer". So, practically speaking, to consent to a payment Mr M needed to make a request with all the details asked for.

- Here, it's not been disputed that a fraudster was able to access Mr M's account and requested the transfer – using the remote access software they convinced him to download. So I don't think he's given his consent, as per the agreed form and procedure, to authorise this transaction.

- I'm also not persuaded that Mr M gave the fraudster permission to consent to the transaction on his behalf. I'm satisfied he thought he was cooperating to secure his broadband. And, given the remote access and what he's consistently said about his screen going blank, that he wouldn't have been aware of the transaction. So I don't think he could've given someone else permission to make it.

- It follows that I'm not persuaded he went through the form and procedure to consent to the payment or gave someone else permission to consent to the payment on his behalf. It was, therefore, unauthorised.

- This means I've gone on to consider whether Mr M failed with intent or gross negligence to comply with his terms and conditions or keep his personalised security details safe.

- I don't think, and it's not been argued, that Mr M failed with intent. It seemed he genuinely believed what he was doing was to resolve his internet's security issues.

- I've gone on to consider whether Mr M failed with gross negligence. Xe suggested that because he failed to keep his personalised security details safe (in line with regulation 72 of the PSRs), that amounts to gross negligence.

- But regulation 77(3) of the PSRs is clear that Mr M is liable for unauthorised transactions if he failed *with gross negligence* to keep his details safe. So it's not enough that he failed. We're instead looking at whether he failed to such an extent that he was *significantly* careless; whether it meant he acted *so far below* what a reasonable person would've done; or *seriously* disregarded an *obvious* risk.

- Here, the fraudster posed as someone from BT, Mr M's genuine provider – and Mr M said they knew his name, phone number and details of his BT account. So I can see why he was persuaded that the person calling was from BT.

- Mr M explained that he was told people were accessing his broadband, which needed to be stopped for security reasons. To sort that, he was asked to download AnyDesk, a remote access software. Given his trust in who he was speaking with,

and that AnyDesk is legitimately used to help people with IT problems, I can understand why he followed these instructions. I think lots of people would've done.

- For the fraudster to transfer money, they would've have needed to log on to his online account with Xe. This involved two-factor authentication – where a code's sent to Mr M's mobile to be entered on the screen. Xe hasn't provided evidence to show that a further code would've been needed to complete the transaction.

- It's not exactly clear how they logged on. I can see from Mr M's browser history that the fraudster visited validator.w3.org. We know scammers commonly use this (legitimate) website to convince their victims that the websites they commonly use, like their online banking, aren't safe and need securing. I think it's likely that something similar happened here – and that's how they convinced Mr M to log on to his online account, so they could 'secure' it.

- In doing so, I don't think Mr M was *significantly* careless. That's bearing in mind that Mr M thought he was dealing with a trusted professional. And that most people aren't experts in cyber security – to understand the genuine signs they're at risk and what steps are needed to keep their internet secure.

- In saying this, I've considered Mr M's testimony that he didn't share the codes he was sent. But it's not clear that he would've needed to. It seems they were only used to log on, so he would've only entered them on the screen. And given that Mr M didn't realise the extent of their control with remote access, I can see why this wouldn't have alarmed him at the time.

- And even if I'm wrong and codes were shared, I'm still not convinced this means Mr M failed with gross negligence. From our experience dealing with similar scams, we know how fraudsters cleverly coach their victims into revealing information, under the guise of securing the website. And I've noted that the codes here aren't clear what they're for, nor is there a warning not to share them.

- So, in all, I don't think Mr M's actions fell *so far below* what a reasonable person would've done that it amounts to *gross* negligence. I conclude Mr M isn't liable for the transaction under the PSRs.

- Xe said its terms and conditions don't suggest its liable to refund victims of fraud and where there was no compromise of its system. But its terms do set out that it'll refund customers for unauthorised transactions in line with the PSRs, which is what I've considered here. I also remind Xe that it can't contract out of its obligations under the PSRs, as per regulation 137.

Putting things right

- Given that Mr M's other bank has already refunded 50% of the amount taken, Xe should refund the remaining 50% (£4,482.66).

- It should pay 8% simple interest per year on this amount, from the date of the unauthorised transaction to the date of settlement (less any tax lawfully deductible).

- In line with regulation 76 of the PSRs, Xe should've refunded this much sooner. That's caused Mr M to worry over his finances, so I also award £75 to reflect distress.

My final decision

For these reasons, my decision is to uphold Mr M's complaint and I order HiFX Europe Limited to settle this complaint as per what I've said under 'Putting things right'.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 21 July 2022.

Emma Szkolar
Ombudsman