DRN-2924802

The complaint and background

Mr M blames Vanquis Bank Limited for the loss of his cryptocurrency due to a sophisticated investment scam.

Vanquis denies liability for what happened, saying that Mr M made authorised payments to a legitimate merchant using the Visa credit card it had issued to him. Accordingly, there were no grounds for a chargeback claim under the Visa scheme; and nor was the bank liable to him under either s.75 of the Consumer Credit Act 1974 or any other grounds.

On 13 July 2021, I issued a provisional decision rejecting this complaint. For completeness, I repeat my provisional findings below:

1. *Not every complaint referred to us and categorised as a cryptocurrency scam is in fact a scam. Some cases simply involve high-risk investments that resulted in disappointing returns or losses. Some crypto platforms may have promoted these products—which are unregulated—using sales methods that were arguably unethical and/or misleading. However, whilst customers who lost out may understandably regard such acts or omissions as fraudulent, they do not necessarily meet the high legal threshold or burden of proof for fraud, i.e. dishonestly making a false representation and/or failing to disclose information with the intention of making a gain for himself or of causing loss to another or exposing another to the risk of loss (Fraud Act 2006).*

2. *Banks and other Payment Services Providers ("PSPs") have duties to protect customers against the risk of financial loss due to fraud and/or to undertake due diligence on large transactions to guard against money laundering (see below). But when simply executing authorised payments, they do not have to protect customers against the risk of bad bargains or give investment advice — and the Financial Conduct Authority ("FCA") has confirmed that a fraud warning would not constitute unauthorised investment advice (see its predecessor's 2012 consultation paper on investment fraud). So, the first question to resolve is whether this particular retailer/trader was a fraudster.*

3. *Mr M's account of what actually happened is slightly vague and, in places, a little self-contradictory — but I do take account of his age and vulnerability. I am satisfied there was no intention to mislead, and that any confusion arises from the inherent nature of a complex new form of digital currency. Piecing everything together on the balance of probabilities, it seems that Mr M was induced, by a supposed crypto wallet or exchange platform called Easy4Click, to purchase some Bitcoin ("BTC"). It appears they persuaded him to purchase the crypto from a legitimate exchange called Jubiter via two Visa-card transactions totalling £1,565, which is the amount Mr M seeks to recover from Vanquis:*

    - *27 Jun 2019: £300*
    - *08 Aug 2019: £1,265*

4. *It appears that the BTC 'wallet address' that Mr M entered on Jubiter's online platform—in which to receive the crypto exchanged for his fiat currency (£sterling)—was in fact fraudulently controlled by Easy4Click rather than being a secure and private address/QR code uniquely assigned to a BTC wallet over which Mr M had control. This is what I*

believe occurred based on Mr M's various statements to Vanquis and us; and in the absence of clear evidence or arguments to the contrary, this will form the basis of my findings of fact on how the funds were lost or stolen by Easy4Click.

5. *If my conclusions above are not persuasively rebutted by either side, I will treat Mr M as the innocent victim of a scam even though the merchant (Jubiter) who actually took the payments and exchanged the crypto was legitimate; and even though the actual theft of the crypto was technically perpetrated by a third party (Easy4Click) after the disputed payments were executed. Mr M later discovered that there was in fact no Bitcoin held by him to trade or exchange back to fiat currency. His Easy4Click 'wallet' or 'online platform' was just a clever digital illusion with nothing in it. In reaching this conclusion, I take into account that:*

    a. *Easy4Click now seem to have vanished without trace;*
    b. *There are many customers online reporting similar experiences. Such evidence, whilst strictly hearsay, can constitute compelling circumstantial evidence if there is enough of it all telling a consistent story;*
    c. *It is common knowledge in the financial services industry—so something of which I can take notice—that certain investments are unregulated, unlicensed and high risk, so merchants trading in them were required by Visa to re-code as a high brand risk. When this happened, in December 2018, many scammers operating in this field changed tack and persuaded 'clients' to purchase real investments (such as crypto) via legitimate third parties, thereby shielding themselves from chargeback claims and putting PSPs off the scent should payment instructions trigger fraud alerts before execution: https://www.fca.org.uk/consumers/cryptoassets;*
    d. *In January 2020, the FCA introduced new powers that allowed it to supervise how firms selling crypto managed the risks of money-laundering and the financing of terrorism, so such brokers needed to register with the FCA by 10 January 2021. And from 6 January 2021, certain crypto-assets were banned from being sold to retail consumers altogether: https://www.fca.org.uk/news/pressreleases/fca-bans-sale-crypto-derivatives-retail-consumers);*
    e. *As a result, I gather that some banks now automatically give customers scam warnings of such practices when purchasing from a coded crypto merchant in an effort to combat the risks of fraud and financial loss.*

6. *Having concluded that this was a scam rather than just a bad bargain or poor investment advice, I now go on to consider four more issues in order to determine the outcome of the complaint:*

    a. *Did Vanquis deal with Mr M's chargeback and/or s.75 claim(s) fairly?*
    b. *If so, were any of the disputed transactions still so unusual or uncharacteristic for Mr M and/or his account that Vanquis's fraud alerts ought reasonably to have triggered some sort of intervention?*
    c. *If triggered, would Vanquis's intervention have made any difference and prevented or reduced the loss?*
    d. *And if so, was Mr M partly to blame for what happened such that it would be fair and reasonable to reduce compensation proportionately?*

Chargeback

7. *Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are*

limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Vanquis) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder.

8. *There was no chargeback claim presented in this case either under Reason Code 53—'not as described or defective merchandise'—or under any other reason code applicable at the time. In my judgment, this omission by Vanquis was not an unreasonable exercise of its discretion on whether or not to pursue the matter against the payee, which the account statements clearly show as Jubiter, not Easy4Click. The Visa chargeback rules did cover this type of high-risk, unregulated trading at that time, as it became included within the scope of Reason Code 53—now falling under 'Dispute Condition Code 13.5'—from 14 October 2017: see Visa Business News, 26 October 2017:*

> *Effective 14 October 2017, issuers may use Reason Code 53 to address cases whereby a binary options (or forex) merchant has imposed obstacles to prevent cardholders from withdrawing funds. This chargeback right is limited to the amount available in the binary option account at the time funds are requested. Issuers cannot charge back more than the original transaction amount, so capital gains from binary options trades cannot be paid out via the chargeback process.*

9. *And from 1 December 2018, Visa's rules changed again to require certain "high-brand risk merchants", such as binary-options brokers, to be coded as Online Gambling Transactions under Merchant Category Code ("MCC") 7995—Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks. Visa Business News dated 6 September 2018 stated:*

> *Visa has discovered that certain binary options, rolling spot forex trading, financial spread betting and contracts for difference merchants are being acquired in markets that do not require licensing or regulate merchant trading platforms. In addition, some of these merchants are selling into countries where local laws prohibit such transactions or require licensing by the relevant financial services authority.*
> *[…]*
> *Global law enforcement, regulators and Visa have received complaints of fraud associated with websites and telemarketers that offer an opportunity to buy or trade binary options, rolling spot forex trading, financial spread betting and contracts for difference. Since 2 July 2018, the European Securities and Markets Authority (ESMA) has prohibited the marketing, distribution or sale of binary options. Since 1 August 2018, the ESMA has restricted the sale and marketing of contracts for difference trading to retail investors for at least three months and may continue to extend the suspension as they study issues with these sectors. The Canadian Securities Administrators has also banned the sale of binary options within its borders. Accordingly, acquirers must take immediate actions to ensure any binary options, rolling spot forex trading, financial spread betting and contracts for difference merchants in their portfolios do not sell into countries that prohibit such transactions.*

10. *Therefore, from 1 December 2018, trading in unregulated/unlicensed investments—of which cryptocurrency is one example (see above)—was a potentially high-risk activity of which banks and PSPs had actual or constructive notice, so could have presented a chargeback if the merchant did not allow the customer to withdraw their funds. (They could also present a chargeback claim if a merchant had expressly promised a guaranteed return contrary to the realities of such high-risk trading. But that was not the case here so far as I can see.)*

11. *Notwithstanding the general principles above, the fact remains that the two Visa payments were made by Mr M to a legitimate crypto exchange, Jubiter. The latter did not defraud him nor steal his money; they did not pass it onto a third party without his consent; nor put obstacles in the way of his withdrawing any funds. It seems to me that*

Jubiter simply did what Mr M asked of them: in return for his Visa payments in £sterling, they exchanged and remitted an equivalent amount in Bitcoin to the (fake) wallet address that Mr M had unwittingly entered into his Jubiter account. Mr M has provided no evidence of what the Jubiter platform stated at the time, but my own research shows that it now clearly warns customers of the following—in a highlighted box under the field for entering "Your BTC wallet address"—when they try to purchase/exchange crypto:

> *Jubiter is only an exchange only [sic] and not affiliated with any 3rd party trading or wallet platforms. Once we have delivered your cryptocurrency to the wallet of your choice the transaction cannot be traced, reversed, altered, or refunded. Create a password at checkout to be able to view your transaction history…*

12. *This supports my view that Jubiter merely executed the currency exchange requested by Mr M — so any chargeback claim against them would be bound to fail under Dispute Condition Code 13.5. Jubiter provided the service, delivered the currency, and imposed no obstacles — so they were entitled to retain the payments that Mr M had authorised. It would be unreasonable to expect a bank to present a chargeback that had no reasonable prospects, particularly as that could incur costs for the bank if the merchant were to defend the claim successfully, which seems likely here.*

13. *For the reasons set out above, I am not persuaded that Vanquis acted unfairly or unreasonably in connection with any rights or responsibilities under the Visa chargeback scheme, so I cannot uphold this complaint on that ground.*

Section 75 of the Consumer Credit Act 1974

14. *Mr M does not appear to have raised a s.75 claim, so I will not go into detail about this issue as, strictly speaking, we can only consider the merits of allegations that a respondent firm has first had a fair chance to consider and resolve informally.*

15. *Having said that, we do have a wide remit, which includes the power to mediate. So, in the interests of resolving this matter "quickly and with minimum formality"—as our enabling statute requires—I shall simply point out that s.75 of the Consumer Credit Act 1974 only gives a debtor the right to pursue a 'like claim' for breach of contract and/or misrepresentation against a creditor as he would have against the supplier of goods or services. But it follows that if Jubiter (the supplier) did nothing wrong, as appears to be the case, there could not reasonably be a successful 'like claim' against Vanquis (the creditor). There is also no right under the 1974 Act to pursue a like claim against a third party (such as Easy4Click) who was not privy to the debtor-creditor-supplier relationship. So, as with the chargeback issue above, I can see no viable grounds under s.75 for upholding the complaint. My comments in this particular paragraph are merely informal observations and do not affect the overall outcome of this case; they are without prejudice to any future claim or complaint that Mr M may bring with regard to s.75.*

Unusual or uncharacteristic activity

16. *Vanquis should be aware of our general position on a PSP's safeguarding and due diligence duties to protect customers from the risk of financial harm due to fraud. We have published many decisions on our website setting out these principles and quoting the relevant rules and regulations. It is unnecessary to rehearse them again here in detail.*

17. *It is common ground that the disputed payments were 'authorised' by Mr M for the purposes of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. This is because they were made by Mr M using the legitimate security credentials*

provided to him by Vanquis. These must be regarded as 'authorised payments' even though Mr M was the victim of a sophisticated scam. So, although he did not intend the money to go to scammers, under the Regulations, and under the terms and conditions of his account, Mr M is presumed liable for the loss in the first instance.

18. *However, taking into account the law, regulatory rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Vanquis 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 its customers were at risk of fraud (amongst other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer; and*
    - *In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment; or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.*

19. *But in the particular circumstances of this case, I do not think it would be reasonable to expect Vanquis to be triggered just by two payments of this size. I accept they were to a new payee; and to a crypto merchant; and that this was a new type of activity for Mr M. But there is no persuasive evidence that they were significantly unusual or uncharacteristic compared with his normal account activity in recent times. It would be too high a burden to expect a bank to become suspicious of fraud or financial crime just on the basis of two payments of £300 and £1,265, which were also a few months apart. For example, those sums are well below the anti-money-laundering thresholds which regulated firms need to monitor.*

20. *Ultimately, Mr M paid a legitimate merchant and in return crypto was sent to the wallet of his choice (albeit due to clever psychological manipulations by a third party). Some banks may now choose not to allow such transactions, particularly using borrowed money—such as credit cards—because of the commercial risks involved. But the fact remains that it was and is not an illegal activity, and many customers now demand faster online payments (which the Regulations are also designed to facilitate).*

21. *There is no evidence that Vanquis had—or ought reasonably to have had—auto-alerts in place at the time just to guard against the risk of fraud associated with some crypto purchases. I therefore conclude that the bank did not act unfairly or unreasonably by not intervening to ask further questions about the transaction or to give Mr M a scam warning.*

22. *In light of my conclusions above, it is unnecessary for me to go on to consider whether any intervention by Vanquis would have prevented or reduced the loss (causation); or whether Mr M was himself partly to blame for what happened (contributory negligence).*

Responses to my provisional decision

Vanquis confirmed on 26 July 2021 that it had nothing further to add to my provisional decision.

Mr M replied on 14 July 2021. He did not accept my provisional decision and submitted that,

before I make my final decision, I should take account of the fact that he was vulnerable at the time he was scammed:

> I was 78 years old with medical problems and I believe that Vanquis should have at least given me some guidance before putting through the second payment to Jubiter. That payment took me up to my credit limit on my Visa card and that should have triggered alarm bells with Vanquis. Up to that time I had paid my account in full each month. After that incident I fell into a situation where I was struggling to pay £70 per month towards paying the debt off.

My findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I understand how upsetting this is for Mr M. I do empathise with his circumstances and am very mindful of the losses he has suffered as a result of this cruel scam. However, I did take account of his vulnerability in my provisional decision; and expressly referred to it in paragraph 3 of that document (see above). Mr M has made no further submissions showing that my provisional findings were legally or factually incorrect, so they must stand.

If this were a decision against Easy4Click as 'respondent', I would clearly be finding in Mr M's favour and ordering compensation on the grounds of their having deceived and exploited a vulnerable consumer. But we have no jurisdiction over Easy4Click (a defunct firm in any event) — so I am limited to determining whether *Vanquis*, as a regulated bank, acted fairly and reasonably in its handling of Mr M's authorised payment mandates. The bank merely executed legitimate payment instructions in a timely manner, as it was required to do under the relevant statutory regulations (and principles of good industry practice, etc).

Vanquis was one step removed from the mechanics of the actual scam, as it were, when sending the monies to a legitimate merchant, so there were practical limitations as to what it could or should have done to protect Mr M from the risk of fraud or financial harm. As I explained in the provisional decision, a bank cannot intervene and disrupt each and every payment that customers authorise using their legitimate security credentials. There have to be reasonable grounds for suspicions; there have to be indicators of fraud which ought reasonably to trigger alerts on the basis of unusual or uncharacteristic account activity.

On the particular facts of this case, the two disputed payments were simply not unusual or uncharacteristic enough, compared with the ordinary account activity, to justify an intervention or scam warning by Vanquis. A bank cannot realistically be expected to stop or question every authorised payment of *c.*£300 or £1,200. Payment services would grind to a halt if that were the case. These sums did not stand out as inherently significant and were well below the transaction thresholds that might ordinarily trigger fraud alarms or require a bank to monitor for money laundering (etc). I have seen no persuasive evidence that Vanquis had actual or constructive notice of anything untoward at the time: Mr M was, on the face of things, simply making authorised payments to a legitimate crypto exchange (Jubiter). This was not illegal activity then or now; it was not to a payee on any national or international alert register at the time; and the sums were within Mr M's credit limit. I do not accept that a bank needs to intervene just because a credit limit is reached. Mr M says he was struggling to repay the debt afterwards but (a) this would not in itself indicate he was the victim of fraud (assuming Vanquis had notice that he was now struggling), and (b) it was by then too late for the bank to do anything in any event: the money had gone and could not be recovered.

I have already accepted that Mr M was vulnerable. But a bank cannot reasonably query all authorised payments just because of someone's age or poor health (assuming it has notice

of the latter). Indeed, that would in itself be unfair and would probably lead to complaints about delays or discrimination. There is no evidence here that Mr M was not of sound mind or incapable of making investment decisions, even high-risk ones. As explained previously, the bank's duty is to guard against the risk of fraud and scams; it is not to give investment advice or protect consumers from bad bargains. And here, there was simply no evidence at the time of the transactions to alert Vanquis to the sophisticated background circumstances which ultimately caused Mr M to divert his payments, via Jubiter, to a crypto wallet controlled by a third-party scammer. In the circumstances, I am not persuaded that Mr M's vulnerability was the proximate cause of the loss or could reasonably have resulted in a materially different response from Vanquis when it was presented with his payment instructions.

My final decision

For the reasons set out above and before, I am not persuaded that Vanquis Bank Limited acted unfairly or unreasonably with regard to these two disputed transactions, so I am unable to uphold this complaint or make any award against the bank.

Under the rules of the Financial Ombudsman Service, I am required to ask Mr M to accept or reject my decision before 29 August 2021.

Mark Sceeny
Ombudsman