Ombudsman Decision
CIFO Reference Number: 24-000268
Complainant: Mrs V
Respondent: HSBC Bank plc, Guernsey Branch

The complainant who I shall refer to as Mrs V complains, in summary, that HSBC Bank plc, Guernsey Branch, failed to protect her from harm when she was targeted by a fraudster who persuaded her to transfer money to a crypto-currency scam. She holds the bank accountable for not having taken steps to identify the possibility of fraud – leading her to incur a substantial financial loss.

Mrs V is represented in her complaint by [] Solicitors. When I refer in this final decision to statements made or evidence submitted by Mrs V, these have been received from her representative.

Background

In summary, Mrs V saw an advertisement purporting to be from a financial advice television show about crypto-currency and after conducting her own online research she decided to invest using company "P" which she believed was endorsed by the television show. Having been reassured by the lack of negative information about P and having carefully reviewed the content, she was assured by the detailed and technical nature of it along with the security regulations the company said that it enforced.

As a result of her enquiries, Mrs V made a payment of £219 as a registration fee to the website. Mrs V then received a call from "R", who told her he was her Account Manager, but was in fact a fraudster. Mrs V has said that she found R to be professional and articulate and immediately had a trusting rapport with him. Mrs V felt that R had provided her with a sufficient

[1] Financial Services Ombudsman (Jersey) Law 2014 Article 16(11) and Financial Services Ombudsman (Bailiwick of Guernsey) Law 2014 Section 16(10)

understanding of the investment before she proceeded with it, was reassured by the knowledge and experience he shared and felt that the returns she was being promised seemed reasonable.

Whilst Mrs V has asserted that R required her to download 'Anydesk' onto her computer so that he had control of her computer, she does not dispute that she made and authorised the following payments using either her Visa or online banking and used one-time passwords herself where required:

Payment	Date	Amount	Beneficiary	Payment method
1	16/06/2023	£219.00	Professor Academy	Debit Card
2	28/06/2023	£1,499.00	Professor Academy	Debit Card
3	14/07/2023	£3,750.00	Professor Academy	Debit Card
4	17/07/2023	£2,000.00	Int'l Plufy Nairobi	Debit Card
5	01/08/2023	£10,000.00	Nexo	Internet Banking
6	03/08/2023	£25,000.00	Nexo	Internet Banking
7	04/08/2023	£10,000.00	Nexo	Internet Banking

Mrs V sent her payments to legitimate websites and was guided by the fraudsters to transfer her balances out of those legitimate website accounts, that is the point at which the fraud occurred.

The fraud was reported to HSBC on 9 August when Mrs V had approached another bank for a loan and when explaining the reason for the loan (that she had been told her investments were losing money and she needed to invest more to protect the investments) she became aware that she had likely fallen victim to a scam.

HSBC were unable to recall payments 5, 6, and 7 which had been authorised by Mrs V to an account in her own name and she was advised to contact the legitimate website company to raise disputes. She later asked HSBC to recall payments 1,2, 3 and 4, but HSBC told her that these did not meet the fraud criteria as she had authorised the payments and there were no Visa chargeback rights in those circumstances.

Mrs V's position is that she was not aware that websites on Google could be fraudulent and that HSBC should have given her more information about the nature of the investment she was making. She is also of the view that HSBC should have done more to stop her making the payments because they were both out of character and were of a higher risk and should have prompted the bank to provide warnings about crypto-currency. Mrs V is of the view that, had the bank intervened in the payments she would have detected the scam earlier and would not have continued to communicate with the scammer or process the payments she did.

Mrs V is seeking reimbursement of the money she lost as a result of the fraud, being £52,468 plus 8% interest and £300 compensation.

HSBC's position is that the payments were authorised by Mrs V to an account she held in her own name and as such they could not be recovered and the debit card transactions did not meet the fraud criteria to process a chargeback with Visa.

The adjudicator did not uphold Mrs V's complaint and concluded that:

- Mrs V had conducted her own research and was confident that she was dealing with a genuine company and had no reason to believe she was being subjected to a scam.
- Having examined Mrs V's bank statements from 6 May 2022 to 5 September 2023, the majority of the transactions were small day to day transactions but there were some large payments between £1,000 and £5,000 and large payments of £10,892 on 16 September 2022 and £15,000 on 27 September. Whilst the international payment to Nairobi may have been a slight change to her spending habits, there were other international payments so it would not appear to be sufficiently outside of her usual spending habits to reasonably expect the bank to identify this international payment as potentially fraudulent. Mrs V's account balance had reduced from £105,124.87 from 6 May 2022 to £55,981.24 on 5 June 2023 before the fraud began, so the reduction in her balance had been gradual over the period, with her expenditure exceeding her income reducing her balance on a monthly basis.
- The first 3 payments Mrs V made with her debit card were not sufficiently unusual compared to her spending habits to have reasonably expected the bank to intervene.

- The 4th payment, which was an international payment to Nairobi, was detailed as such on her statement, which did not cause Mrs V concern or to question the legitimacy of the payment she had made.
- When Mrs V made the final 3 payments via online banking she was guided to select the incorrect payment reason by the fraudster and when presented with a fraud warning which covered this eventuality, it did not raise concern with her, and she proceeded with the payments anyways.

Mrs V did not accept the adjudicator's recommendation, and her representative asked for a final decision on the following basis:

"*Although it is recognised that our client had previously conducted large transactions, the pattern and nature of the payments associated with the scam were out of character. These payments were made to entities outside of our client's regular transactions. Such activity should have been identified as unusual, prompting a more thorough investigation by HSBC. The bank ought to have directly contacted our client to confirm the authenticity of these transactions, particularly considering the nature and substantial size of the payments made within a short timeframe*."

The complaint has now been passed to me for a Final Decision

Findings

I have considered the available evidence and arguments to decide what is, in my opinion, fair and reasonable in the individual circumstances of this complaint.

The starting point is that it is the bank's principal duty to make the payments its customers ask it to make. Banks in Guernsey are also under a regulatory obligation to have systems and procedures in place to prevent fraud. While CIFO must note relevant laws, regulations and codes of practice in determining what would be fair and reasonable in the circumstances of an individual complaint, CIFO does not directly apply UK law, regulation, or codes of practice to Channel Islands complaints. The various UK regulations, thematics and guidance that Mrs V has referred to are not directly applicable to her complaint. Mrs V's account in Guernsey is subject to regulations set out by the Guernsey Financial Services Commission (GFSC). The GFSC's Code of Practice for Banks was published under section 41 of the Banking Supervision (Bailiwick of Guernsey) Law 2020, and requires a bank, amongst other things, to '*have in place* *comprehensive risk management processes to identify, measure, monitor and control material risks'* and also requires that '*procedures should be I place to counter external fraud and other financial crime'*. It is these laws, regulations and codes that CIFO must take note of.

CIFO is also required to take into account good industry practice in deciding what's fair and reasonable. It may be good practice for banks to intervene where, for example, the bank is aware of features of a transaction (or a series of transactions) which indicate that a customer may have been targeted by fraudsters, therefore I have considered the following questions:

1. Given what it actually knew about the payments, should the bank have raised with Mrs V the possibility that the investment was not genuine?

2. Was there anything about the nature of the payments which ought to have led the bank to ask further questions of Mrs V before completing them?

3. If HSBC had acted differently before completing the transfers, would Mrs V's losses have been avoided or reduced?

In some cases, a bank might know more about some aspects of a transaction than its customer does, for example, it might have received information about fraudulent activity on a receiving account. That is not the case here and HSBC did not know more about the payments than Mrs V did. In reality, it knew less. The bank knew the identity of the recipients, but it had no information about the circumstances in which Mrs V had decided to invest or to make the payment or about the individuals involved.

Where the payments were being made by Mrs V to a legitimate digital platform, the bank did not know that Mrs V might transfer the funds onward to a crypto-currency investment. I don't believe that HSBC had any specific knowledge about the payments, which meant that they reasonably should be expected to have intervened.

I have therefore considered the second point, namely whether the bank should have done more before completing the transactions. I do agree that the last three payments were somewhat out of character, being of high value and paid over a short period of time, but this was not a case where the bank had done nothing at all.

When Mrs V made payments 5, 6 and 7 she was required to select a reason for the payments on each occasion and a fraud warning relevant to that selection was shown. Mrs V at the request of R, chose '*Buying goods and services'* as the reason for the payment, despite the more suitable investment option being available to her. Had she selected the investment option she would have likely received more specific warnings, specifically about crypto-currency risks, but by proceeding as she did, Mrs V received the following warning (<u>my emphasis</u>):

> "***Caution – This could be a scam****.*
> *<u>If someone has told you to mislead us about the reason for your payment and/or choose the wrong payment type, stop, this is a scam.</u>*
>
> *Fraudsters may advertise products, goods or services on social media or other online marketplaces. In some cases, they even set up and use legitimate looking websites.*
>
> ***What you need to do before making the payment:***
>
> - ***Stop*** *and* ***think*** *– does this seem right? Is the offer for a limited time or feel too good to be true?*
> - ***Don't*** *make the payment if you're asked to pay by bank transfer rather than using a secure way to pay e.g a credit or debit card, which gives more protection against fraud.*
> - ***Don't*** *make the payment if you are asked to send it differently to how you normally would.*
> - ***Beware*** *of false websites and reviews and thoroughly research the seller online using trusted sources before sending any money.*
> - *If you're paying for a high value item like a car, make sure you physically see it before making the payment.*
> - *If you've been asked to purchase via a website always type the address into your web browser and be wary of using links in unsolicited emails. Visit our* ***security centre*** *for more guidance on what you should check before making payments.*
>
> ***Important***
>
> ***By choosing to continue, you agree you've read our warning and are happy to proceed. You accept that HSBC is not liable and may not be able to recover your payment if it is sent to as fraudster's account. If you're unsure, please stop immediately.***"

In this case I think the warning from HSBC was sufficient for Mrs V to stop and think about why she had been told to select the wrong reason for the payment and to alert her to both the possibility that she was being subjected to a scam. Mrs V was required to select '*Continue*' or '*Stop payment'* after seeing the warning and on all three occasions she acknowledged the warning and selected '*Continue*'.

Mrs V believes that HSBC should have stopped the payments and made more thorough investigations about the payments she was making and should have provided her with sufficient information about the nature of the investment she was entering into. I do not agree. The bank's principal purpose in making enquiries around a payment is to check/confirm that the customer is satisfied that the payments they are making are genuine and as intended. It is Mrs V's obligation to undertake her own due diligence and to understand the investments she was making. I do not consider that the bank's duties or obligations extend to looking into the background of an intended ultimate beneficiary on behalf of a customer before processing a customer-authorised payment.

Even if the bank had stopped the payments, Mrs V has confirmed that she was satisfied that she was dealing with a legitimate company and was investing in a genuine opportunity. The sophisticated website, the security policies that she saw, the reasonable profits she was receiving, the good business practices being implemented and the professional and trustworthy approach she experienced, all reassured her that her money was safe and the investment was legitimate. In my view, on the balance of probabilities, any intervention from the bank at that time would have been unlikely to prevent Mrs V from proceeding with making the payments.

Mrs V was confident that the investment was genuine and as such I do not believe that the bank speaking to Mrs V before releasing any of the payments would have made any difference to the outcome here. The fraud warning she accepted did not alert her, nor did she react when it was clear from her statement that she had unwittingly made an international payment to Nairobi.

The fraud came to light at the point in time that Mrs V had run out of money to invest further and this is when the fraudsters began to tell her that the value of her investment was falling and would continue to do so if she did not invest more. When she approached another bank to obtain a loan to continue to invest, they alerted her to the possible fraud. At the time Mrs V made the payments she could see a credible website showing returns and was not receiving pressure to invest greater sums, as such I do not believe that losses would have been avoided.

HSBC were unable to process recalls on payments 5, 6 and 7 as they were made to an authorised account in Mrs V's own name and she was correctly referred to the website to report the fraud. I therefore cannot conclude that HSBC could have done any more to recover those payments.

HSBC concluded that payments 1, 2, 3 and 4 fell outside of the criteria to complete a chargeback, and whilst I agree with the adjudicator that it would have been better for HSBC to refer the chargebacks to Visa, I am satisfied that they were unlikely to succeed. The payments were duly authorised by Mrs V to the legitimate websites and Mrs V received the services she paid for. The fraud occurred subsequently and therefore did not fall into any of the chargeback categories which primarily relate to a payment being made without the customers' knowledge or the goods or services not being received or as described.

I am very much aware that what I have set out above will come as a profound disappointment to Mrs V. However, for the reasons that I have explained, I do not consider that it would be fair or reasonable for me to impose a liability on the bank for the payments that Mrs V herself authorised HSBC to make where there were no obvious warnings the bank should have heeded.

Final Decision

My final decision is that I do not uphold this complaint.

Douglas Melville
Principal Ombudsman and Chief Executive

Date: 22 December 2025