Before the Arbiter for Financial Services

Case ASF 085/2024

PI

('the Complainant')

vs

HSBC Bank Malta p.l.c.

(C 3177)

('the Service Provider, 'Bank' or 'HSBC')

Sitting of 24 January 2025

The Arbiter,

Having seen the Complaint filed with the Office of the Arbiter for Financial Services ('OAFS') on 24 April 2024 against HSBC Bank Malta plc ('the Service Provider, 'Bank' or 'HSBC'), where the Complainant claimed that within the span of a few days during June/July 2023, she fell victim to serious online investment scam where she ended up losing her savings of EUR70,100, following the transfers she made from her HSBC bank accounts to a fraudster.[1]

HSBC was her primary bank where she received her salary and with whom she held her house loan. The funds were transferred principally from her HSBC savings accounts to her own Revolut account. These were then transferred to Binance and then to the fraudsters.

The Complainant explained her story began in July 2023 after initially investing Eur 250 (in February 2023)[2] to trade as a beginner on an online trading platform

[1] Complaint Form on Page (P.) 1 - 7 with extensive supporting documentation on P. 8 - 100

[2] P. 113

under the guidance of a certain Matthew McBride (as a representative of a UK company, *Edge Finance Ltd*), who appeared to offer all the necessary market guidance. She noted that after several months, he gained her trust as she saw trading positions closing at a profit on the platform. McBride made her feel guilty for not trading actively and not replying to him due to work commitments.

She further explained that one day, McBride informed her that she had made big profits given that crypto had risen to a peak, but that for the profits to be withdrawn, she had to open an account through Binance for tax purposes. The Complainant stated that she was informed that if she did not act quickly, she might end up in trouble with authorities, and all her assets might get frozen.

The Complainant further noted that she was very afraid but, at the same time, thought McBride was truly genuine as she had searched the company, *Edge Finance Ltd*, that McBride told her that he represented, and had found this company on the UK FCA's register. She thus believed that she was dealing with an FCA-registered company.

She followed McBride's advice and started communicating with him almost daily to guide her on how she could withdraw her money. The Complainant explained that an account was opened with Binance where McBride first transferred some funds as a test (which she truly received) and then told her that he would proceed to transfer the huge profits made.

The Complainant explained that from that point onwards, she started receiving communications from (someone impersonating) Binance where she was notified that there were some pending funds for withdrawal but that she had to first pay for liquidity checks before the money was released.

The Complainant noted that she had also searched about Binance and noticed that their website seemed secure and serious. She had also replied to their email by challenging their requests and even had a call at one point to clarify the next steps. The Complainant noted that little did she know, however, that the emails/ calls she was receiving were not from the real Binance team.

She claimed that the email communications were from a fake email address created by the scammers pretending to be Binance.

The Complainant further explained that she followed the orders to convert money into Bitcoin (BTC) and transferred real BTC through her real Binance account (to the scammers). It was pointed out that she discovered about the scam only after receiving a fake letter from the FCA asking her to pay a large amount in tax. The Complainant noted that she was aware that the FCA did not normally deal with tax, and she phoned FCA, who confirmed the very sad news that she was dealing with a scammer.

It was further noted that a report was made to HSBC on the same day she detected the fraud, and a case was opened with the fraud team. The Complainant claimed that the Fraud Team, however, never contacted her directly despite the severity of her case and the losses incurred.

Alleged shortfalls as explained by the Complainant in her Complaint[3]

The Complainant claimed that despite she was transferring the funds to a Revolut account held in her name, it was clear that HSBC had no controls to protect her from serious fraud.

She submitted that even if she had authorised the transfers, she was in a panic mode, given that she was constantly being threatened to act quickly. The Complainant pointed out that she was being told that, otherwise, she would get in trouble with the Authorities.

The Complainant submitted that, unfortunately, at no point in time did she receive a risk warning from HSBC employees and/or a simple call. She claimed that she did not even receive an automatic in-app risk warning that would have helped her open her eyes in those difficult circumstances. The Complainant noted that she could barely sleep those days and, for this reason, it took her some time to escalate her case to the Arbiter.

She submitted that, based on her historical payment patterns and behaviour, she was a very conservative client and that, save for most of her salary, she did not transfer such large amounts of money in short timeframes. The Complainant further claimed that she had been an HSBC customer for many years, so there was sufficient historical data on her accounts.

[3] P. 4

The Complainant submitted that it was clear that HSBC had no controls over monitoring the payment patterns of cardholders to help detect abnormal activities, be they authorised and/or unauthorised.

She claimed she was a victim of a serious scam and her family was still struggling and trying to recover financially from the losses incurred in July 2023. The Complainant submitted that if HSBC had adequate controls in place (be it an employee calling prior to approving the various large transfers, or at least a simple automated risk warning), she would have perhaps realised about the scam before losing all the money she had in her HSBC accounts.

Remedy requested

The Complainant wants to recover her lost funds of EUR 70,100.[4]

Having considered, in its entirety, the Service Provider's reply,[5]

Where the Service Provider, in its response of 16 May 2024, explained and submitted the following:

'*That the Complaint is unfounded and ought to be rejected because of the following reasons:*

1. *The Complainant, who happens to be a senior XXX officer working in an insurance company has in June 2023 and July 2023 effected a number of payment transactions on her own accord and free will to her account with Revolut amounting to EUR 70,100;*

2. *The Bank is not the correct defendant of the case. Through her various payment instructions to the Bank for transfer from her HSBC account to her Revolut account, the Complainant has manifested her resolution and clear intent to credit her own account with Revolut from where funds were then debited by her to buy cryptocurrency from a third party. It is at this latter stage, i.e., when she decided to transfer funds from her Revolut account to a third-party beneficiary that the Complainant needed to assess the danger of transfer of funds from her own account to a third party. Any prior warning that may have been provided by the Bank to*

[4] P. 4
[5] P. 107- 108

prompt her about the beneficiary of the payment would not have prevented the Complainant from deciding to credit her own account with a third-party payment service provider;

3. *Without prejudice to what is stated above, from the chats provided by the Complainant herself, it is clear that she knew what she was doing, and she had been in contact with* ***the third parties she chose to negotiate with at least since March 2023*** *– i.e., months before the contested payments transactions of June and July 2023 took place. She also seems to have persistently withdrawn and deposited funds in her HSBC credit card account throughout June and July 2023 indicating repetitive behavior unlikely to suggest that she was under threat. As a result, Complainant's claim that she effected the contested payment transactions in 'panic mode' is untenable;*

   That in view of the above, the Bank submits that the complainant's claim is unjustified in fact and at law and that consequently all Complainant's demands are to be rejected with costs to be borne by the said Complainant'.[6]

Preliminary

Plea that the Bank is not the Correct Defendant

In its submissions of 16 May 2024, the Bank raised the plea that it was not the correct defendant given that the payments done by the Complainant from her HSBC account went into her own account with Relovut and that it was from the account held with Revolut that the payments were in turn eventually made to the fraudster.

The Bank claimed that it was, at that stage, when making the transfers from Revolut to the third party, that the Complainant had to assess the danger of the transfers. It submitted that any prior warnings provided by HSBC at that stage would have not prevented the Complainant to proceed with the payments to third parties.

[6] P. 107 - 108 (Emphasis added by the Service Provider).

In its final submissions, HSBC reiterated that the transfers made out of her HSBC account were fully authorised by the Complainant herself and only involved transfers to another regulated bank, Revolut. HSBC pointed out that the transfers were fully authorised and initiated from the usual IP address/es and did not trigger any indication of elevated risk.

The Bank reiterated that there was no fraud scenario at the point of transfer to Revolut and that HSBC was not involved, in any way, in the transactions that the Complainant chose to make from her account with Revolut to third parties. For the said reasons, HSBC submitted that any claims for damages allegedly suffered by the Complainant should be addressed to Revolut, not HSBC.

The Bank further submitted that the lack of jurisdiction by the Arbiter on Revolut should not be utilised to condemn the Bank, which was an innocent party.

The Arbiter considers that the said plea raised by the Bank is an aspect which relates more to the considerations about the merits of the case. There is no doubt that the various payments in question were originally made from HSBC's account. The Arbiter, therefore, has to consider whether there were any shortfalls on the part of HSBC with respect to the said payments as so alleged by the Complainant. The Arbiter shall only review and consider the alleged shortfalls that strictly relate to HSBC and not to any other third parties and shall next proceed to consider the merits of the case accordingly.

The Merits of the Case

The Arbiter will decide the Complaint by reference to what, in his opinion, is fair, equitable and reasonable in the particular circumstances and substantive merits of the case.[7]

The Arbiter is considering all pleas raised by HSBC relating to the merits of the case together to avoid repetition and to expedite the decision as he is obliged to do in terms of Chapter 555[8] which stipulates that he should deal with complaints in '*an economical and expeditious manner'.*

[7] Cap. 555, Art. 19(3)(b)
[8] Art. 19(3)(d)

Considerations

Background about the scam

The Complainant claimed McBride was an impersonator and false representative of *Edge Finance Ltd*.

As per the extracts of the various mobile text messages exchanged between McBride and the Complainant from March to April 2023,[9] the Complainant was initially guided by McBride to execute certain specific positions (buy/sell instructions) on currency pairs (forex trading) with her initial investment of EUR250. The instructed trades started closing at a profit and the Complainant was, at the same time, being provided with various market updates. These were seemingly attempts to lure her into thinking she was dealing with a professional person and how easy it was to profit from the guidance provided. She was also regularly notified by McBride that she was missing various opportunities with McBride also occasionally trying to get her to invest more money.

Given the Complainant's lack of availability to continue doing the online trades, McBride informed her in April 2023 that he would start opening positions himself on her account from that point onwards.[10] The Complainant did not appear to be much active on her account in subsequent months (as indicated by McBride in one of his text messages).[11]

In June 2023, the Complainant was contacted by McBride, who notified her that he had put her account on *'special projects'* involving crypto, which yielded huge profits (whilst at the same time luring her to invest more money).[12] McBride claimed that her account had increased to EUR95,000.[13]

The Complainant was encouraged by McBride to open an account with Binance to purportedly speed up the profit transfers and for tax related reasons. A *'test withdrawal'* was seemingly also done to further gain her trust and alleviate suspicions.[14] She then started receiving communications from a fake Binance

[9] P. 22 - 50
[10] P. 36
[11] P. 37
[12] P. 38
[13] P. 41
[14] P. 39 & 41

email account (ending '*@binance-support.ltd'*) in coordination with communications from McBride and others.

In order to receive the alleged substantial profits, the Complainant was asked to do various substantial transfers and payments first. She was deceived into thinking this was part of the purported validation of her accounts, with various excuses also being gradually but frequently made within short periods of time, demanding payments before her purported profits could be released. Such excuses ranged from the 'need' to do a *'liquidity check',*[15] for *'insurance purposes'*,[16] to *'unfreeze funds*',[17] for *'creating a history of transactions'*,[18] for *'cashflow purposes'*.[19]

For example, with the excuse that she needed to first create a history of transactions, she was requested to do three transfers, a *'First Transfer'* of USD2,500, a *'Second Transfer'* of USD10,000 and a *'Third Transfer'* of USD30,000. To alleviate concerns and gain her trust, she even received back the first and second transfer. The third transfer, which was the largest payment, was however not received back as explained by the Complainant.[20]

According to the information provided, the Complainant ended up paying and losing (over USD 71,000) between June and July 2023 as follows:

- Approx. USD 7,200 (EUR 6,900 - two payments of around USD 3,600) in Liquidity Checks (where the Complainant was requested to re-submit the payment with the excuse that the exact conversion of USD to BTC was not made);[21]
- USD 9,000 (EUR 8,000) in an Insurance Payment;[22]
- USD 30,000 for a Third Transfer requested to create history with "Binance";[23]

[15] P. 18 & 48
[16] P. 18 & 55
[17] P. 18
[18] P. 52
[19] P. 19 & 57
[20] P. 55 & 64
[21] P. 60, 64 & 114
[22] *Ibid.*
[23] P. 54, 64 & 115

- USD 25,000 requested Cashflow Payment with "Trust Wallet".[24]

An attempt was also made on 14 July 2023 to try and extract a substantial *'international tax payment'* of EUR 50,000 from the Complainant for the final release of profits. At that point, the Complainant realised about the scam.[25]

Veracity about the asserted scam

It is noted that, in its final submissions, the Bank raised the point (not previously raised) that:

> *'… the Bank has been provided with screenshots from a mobile phone showing a number of WhatsApp messages. The Bank cannot verify whether these WhatsApp messages are complete or genuine ...'*.[26]

However, no reasonable doubts have emerged (and neither were they raised in the Bank's reply or hearings held) that the Complainant was not a victim of a scam.

The Arbiter would like to point out first that he has no reason to doubt the veracity of the Complainant's claims and is satisfied that there are no reasonable doubts on this aspect, even on the balance of probabilities, that the Complainant was not a victim of a scam.

Consideration has, in this regard, being given to various factors including: the particular circumstances of this case; the testimony and the evidence produced; the nature and credibility of the events outlined in the complaint; the Complainant's profile who occupied a senior position in a local insurance company and who was thus well aware of the consequence of false allegations or testimony; the report made by the Complainant to the police dated 24 July 2023;[27] the sworn testimony and the Complainant's affidavit on the fraud case;[28] extracts of communications with the scammers;[29] statements from Revolut (as requested in the Arbiter's decree of 13 January 2025)[30] which corroborated the

[24] P. 60, 64 & 115
[25] P. 60 & 61
[26] P. 191
[27] P. 63 - 65
[28] P. 123 - 125 & P. 112 - 120
[29] P. 22 - 61
[30] P. 195

Complainant's claims of transfers to Binance;[31] and correspondence exchanged with the Bank[32] including the unsuccessful recall attempts made.[33] These all reasonably support the claim of fraud and that the Complainant fell victim to a sophisticated scam.

Payments subject to this Complaint and other background

The following is a schedule listing the payments subject of this Complaint:

TABLE A

Date[34]	*MASTERCARD CARD EURO*	*SEPA OnLine EURO*	*Bank Account*
30.06.2023	700		IBAN …82
30.06.2023		8400	JOINT SAVINGS
30.06.2023		1500	JOINT CURRENT
30.06.2023		1500	SAVINGS …50
01.07.2023		1500	JOINT CURRENT
01.07.2023		1500	SAVINGS …50
05.07.2023		5000	SAVINGS …52
06.07.2023		8000	SAVINGS …52
07.07.2023		18000	SAVINGS …52
11.07.2023		24000	SAVINGS …52
TOTAL	700	69400	

[31] P. 197 - 203. The official statements from Revolut reflect the multiple transactions to Binance for a total of EUR 71,150 that were undertaken over a short period of time during end June 2023 to mid-July 2023 as outlined by the Complainant in the attachment to her Complaint (P. 21).
[32] P. 8 - 15
[33] P. 168
[34] The actual sequence of these payments may be slightly different from what is shown in this Table as the Revolut Satement submitted (p. 200) show the four payments of €1,500 being received by Revolut before the payment for €700 and €8,400.

The Complainant claimed a loss of EUR 70,100 due to the said payments – a substantial part of which (EUR 58,000) were mainly made from the Complainant's personal savings accounts held with HSBC (ending with numbers 50 and 52).

These payments were made to a Revolut account held in the Complainant's name from where transfers were then made to another account held with Binance[35] from where they were converted to crypto and transferred to one or more crypto wallets held by the fraudster.

Apart from these payments, it seems that around that time, the Complainant also affected or tried to affect a number of payments to her Revolut account, which are however not the subject of this Complaint:

TABLE B

DATE	MASTERCARD CARD EURO	SEPA OnLine euro	Payment succeeded or refused
28.06.2023	3000		Refused
28.06.2023	1500		Succeeded
28.06.2023	1500		Refused
28.06.2023	1500		Refused
28.06.2023	1200		Refused
28.06.2023	1500		Refused
28.06.2023	1500		Refused
29.06.2023	1500		Succeeded
29.06.2023	1500		Refused
18.07.2023		25000	Succeeded

[35] P. 20 - 21 & P. 197 - 203

It seems that only in three cases did the payment succeed. However, the last payment for €25,000 was not indicated as having been transferred under the control of the fraudster and, for this reason, does not form part of the claims made under the Complaint.

The two successful payments each for €1,500 are included in TABLE A with slightly different dates. The said payments or attempts for payments however, cast a light on the state of mind of the Complainant at the time she fell victim of the scam.

When the Complainant realised that she fell victim to a scam on 19 July 2023, she asked HSBC's help and eventually made a formal complaint[36] where she asked the Bank to refund the money she lost as she claimed that the Bank did not have proper systems in place which would have prevented her from falling victim to the scam.

The Bank refuted the said claims claiming *inter alia* that the payments were approved by the Complainant herself and made to her own account with another licensed bank, Revolut.[37]

Hearings

During the first hearing of 3 September 2024, the Complainant's lawyers, who had just been recently appointed by the Complainant, asked to be given further time to *inter alia* present an affidavit by the Complainant and present other documents before the next sitting. The request was acceded to by the Arbiter following also the Bank's no objection to the said requests.[38]

The Complainant subsequently presented an affidavit which explained in more detail her ordeal and complaint.[39]

The cross-examination of the Complainant was then held during the hearing of 21 October 2024. During the said sitting, the Complainant testified that:

[36] P. 8 - 15
[37] P. 15
[38] P. 109
[39] P. 113 - 122

'I say I have tertiary education, and I work in the insurance industry, but I have no experience whatsoever in trading, in cryptocurrency, etc.

I graduated in XXXX and XXXX, not in insurance. But then, I started working in insurance.

I do not work in the XXX sector of XXX; XXXX. I am in the XXXX side of things in my insurance company.

Asked how I met this person to whom I decided to make such payments and make such investments with, I say that as already explained in my affidavit, there was an advert that I registered my interest in and I was introduced to this person who I searched and found out that he was representing a company, Edge Finance, which was registered in the FCA register. I know that the FCA are very strict in terms of authority, and I thought, of course, that this was a legitimate company. And this is why I felt comfortable to communicate and deal with this.

Asked whether I undertook any due diligence, I say that I am a non-experienced investor, I am not professional in this, my due diligence consisted of searching this company and it appeared to be listed in the FCA register which is a very strict authority indeed. I say that I felt safe that this company was listed in the FCA register.

Of course, I had no idea at the time that clone companies exist. I only discovered that these entities exist after I have unfortunately experienced this myself.

The Arbiter refers to point 25 of the affidavit (page 118 of the process) to the table which provides details of the payments totalling €70,100.

Asked by the Arbiter to clarify what I mean by 'a total of €95,000', I say that the whole scam started towards the end of June when this scammer sent me an email shocking me as initially, I had invested €250 back in February and in the meantime between February and June nothing much was happening. He was slowly, slowly building a relationship with me, providing me with market updates, etc.

Regarding the €95,000, I say that they were the savings at the time. I had withdrawn from my account the total of €95,000 but then, the last €25,000, were never transferred to the scammer.

The Arbiter says that it seems that these €25,000 (shown in the table dated 18 July 2023) is part of the total of €70,100.

I say that the €70,100 do not include the last figure of €25,000.

Asked by the Arbiter since I have a tertiary education, I work in XXX and have a sizable salary, and I invested €250 in February and somebody tells me that by June I will make a profit of $90,000, does this not tell me that something is not right, I say that he did not tell me this before. I just invested €250. I was not expecting that amount. In fact, when he sent me that news by email, I was shocked but now I say how I could believe something like that.

The thing is that he was threatening me. He told me that I had this amount and that if [I] did not act then, my account will be frozen, and I will have problems with the authorities.

It is true that I have tertiary education and a substantial salary, but this does not mean that I am an expert in this sector.

Asked by the Arbiter what did I think the police would do to me, I say, to be honest, I was not thinking about the police. I was thinking of other authorities in the crypto world, in the financial services. My mind was all over the place at that point."[40]

The Bank's representative also testified during the said hearing to present the Bank's submissions and proofs. HSBC's representative stated:

'I say that I have prepared an affidavit, which I will go through, which was prepared from the files and from the investigation made internally.

[The Complainant] transferred money to her Revolut account in 2023. From a PSD perspective and from CBM Directive 1's perspective, it seems that [the Complainant's] intention was to make these payments from her account at

[40] P. 123 - 125

HSBC to another account with another bank and the bank executed her requests as per her instructions.

The bank had no visibility or foreseeability on the transactions that happened on the other side, that means on her Revolut account and from that aspect the bank considers that the transactions from her HSBC account were all authorised.

The bank considers that in this instance there was a no fraud scenario as the money was transferred to what appeared to be a legitimate destination, that is, her accounts with another provider.

Prior to all these transactions, it appears that [the Complainant], from her account ending …50, had affected two large transfers: one on 11 February 2022 for the amount of €1,700 from her account to Revolut, and another one on 1 November 2022 for the amount of €500.

[The Complainant] was familiar with Revolut bank and from an analysis performed on [the Complainant's] account, it seems from the top-up to her Revolut transactions, it showed that she switched from Revolut to SEPA payment.

This happened because on 28 June, [the Complainant] transferred €3,000 which were declined due to her card parameters, and then she tried to affect a transfer for €1,500 which was then approved; and she kept on trying to process another €1,500 . Afterwards, however, and an additional €1,200 on the same date but these transactions were not authorised due to her card parameters.

On 29 June, she processed again another transaction of €1,500 and this was approved; but the second attempt for another €1,500 top up to Revolut was again declined due to parameters.

(Here [the Bank's representative] showed on screen a table with all the transfers [the Complainant] tried to affect with her card).

It is important to note that in this respect, [the Complainant] opted to transfer through SEPA. When she opted to transfer through SEPA, the updated balances of her transactions were immediately visible. The

outward transfers were all done from account ending ...52 in July 2023. It was noted that with regard to her last Revolut transfer on 18 July 2023, this transfer was for €25,000 and [the Complainant] did not have sufficient funds for such transfer and she topped up this account from three other accounts that she had with us.

It should be emphasised that two of these accounts were in the joint names of the complainant and a third party who also had full visibility to Internet banking.

We know [the Complainant] as an insurance professional earning quite a substantial salary. And on 9 June 2021 she was eligible for Premier status with HSBC. And during such upgrade from her previous status to one of Premier, [the Complainant] would have been made aware of her transaction parameters.

Also, I would like to refer to the general Terms and Conditions of savings and current accounts which advise our customers that there are transaction llmits imposed on our accounts and such parameters may be modified also by the customer at their own discretion by either going to a branch or through Internet banking or through home banking.

It is important to highlight that HSBC Malta does not allow transfers to Binance. In fact, the bank has blocked Binance for a long time prior to [the Complainant's] transactions. Therefore, had she tried to transfer this money direct from HSBC, she would not have been allowed to transfer to Binance.

Also considering that with regard to Binance, there has been significant media coverage when the MFSA had warned about Binance transactions.

On 23 June 2023, the bank had sent an email to the email address of [the Complainant] which she has got registered with us: ...

This email was sent to her email address and did not return undelivered. So, it is deemed to have been received by [the Complainant].

There was a section in this email: 'Keep yourself safe from scammers and fraudsters.'

This email also included, 'We would like to remind you to be always vigilant and ignore anything which seems suspicious or too good to be true.'

And there is other information.

I would also like to present this email that was sent to the complainant after this hearing.

[The Complainant] was not subscribed for the free SMS alerts so we could not have sent you any SMS alerts.

However, even if [the Complainant] had this subscription for these free alerts, the SMS alert would have been sent to her once the transaction has been authorised.

With regard to the table I showed on screen earlier with all the transfers that [the Complainant] attempted with her card, I say that this table covers payments from 1 April 2023 till 31 August 2023.

The Arbiter states in point 25 of the affidavit, there is a table with the payments complained of and if he understood correctly, I made reference to payments which are not part of the complaint which start from 30 June and it seems that the payment of 30 June for the amount of €700 there is written 'Paid by debit card Premium Mastercard'; following that they were made by bank transfer, some of them from different accounts up to 1 July. There was one big payment from ...51 (a joint account) and then, from 5 July, they all came out of ...52. I say, yes, they were done by SEPA.

Asked by the Arbiter whether this table of payments is correct, I confirm that the table of the payments she submitted is correct.

I say that it corresponds with her records.

I say that the only reference I made to the joint account was that when she tried to affect the transfer of €25,000 on 18 July, the transfer failed to go through and due to insufficient funds, she credited her account ending ...52.

The Arbiter points out that the afore-mentioned payment eventually went through but it did not go to the scammer and is therefore not part of the complaint.

Asked by the Arbiter what were the transaction limits for accounts ending ...52 and ...51, I say that I would not know the transaction limits but we can check.

The Arbiter states that what he is trying to establish is that there was a payment of €24,000 and €25,000 and since that payment was not stopped, he asks whether there was a transaction limit of €25,000 on those accounts, I say that probably since [the Complainant] was a Premier Customer, Premier Customers would have larger parameters available on their internet banking.

So, these payments were not subject to an increase in limit. She did not need to call.' [41]

Following the sitting of 21 October 2024, HSBC presented the following documents:

1. A copy of a communication sent to the Complainant by the Bank through a circular dated 23 June 2023.[42] Reference was particularly made to the section titled ***'Keep yourself safe from Scammers and Fraudsters'***;[43]

2. A copy of the General Terms and Conditions – Current, Savings & Card Accounts for Individual and Micro-Enterprises[44] where reference was particularly made to the section ***'D.4 Fraud Prevention and Compliance with Laws'***;[45]

3. A table which was referred to by the Bank's representative during the hearing of October 2024 reflecting the payments that the Complainant did, or tried to do, with her card between the 19 June and 25 July 2023.[46]

The Bank's representative was cross-examined on 13 November 2024, during which the representative testified the following:

[41] P. 125 - 128
[42] P. 131 - 136
[43] P. 135
[44] P. 137 - 161
[45] P. 151 - 152
[46] P. 162

'Asked whether it is correct to state that HSBC never informed its clients that it was not going to be allowing transfers to Binance, I say that, no, HSBC does not inform customers but as soon as there is an alert or something, HSBC takes all the necessary precautions.

With regard to Binance, the specific merchant, there was a circular issued by the Malta Financial Services Authority stating that Binance is not secure and asking to stop payments to Binance. I think this was around 2020.

Asked whether HSBC informed its customers of this circular, I say I wouldn't know.

It is being said that on the 25 February 2023, [the Complainant] had affected a payment of €250 directly from her HSBC card to Easycrypto4U.com as appeared on her statement which was the initial transfer that she had made.

Asked whether it is correct to state that since this payment had passed through, the bank considered this receiver account, Easycrypto4U, to be a legitimate destination and a legitimate transaction, I state that a transfer to any merchant, unless there are any negative news or information in the public domain which we believe to be serious enough to take action, we leave every merchant because what you are saying is that if I go and buy something from a new shop, will I be stopped?

I say, yes, HSBC allowed this transaction as it had been verified by [the Complainant]. She wanted to do it.

It is being said that on 28 June 2023, there was a transaction for €3,000 which initially [the Complainant] tried to affect through her card and asked whether it would be correct to state that the only reason the transaction was blocked was because the amount of €3,000 exceeded the daily parameters for card payments, I say that the transaction of €3,000 was made from her bank account at HSBC Bank Malta to her Revolut account. That particular transaction of 28 June 2023 was declined because of card parameters.

Asked whether it would be correct to state that on 28 June 2023, the bank had different parameters in place for card holders, for card payments and for SEPA payments, I say that those are two different kinds of payments so their parameters would be different. The parameters are different for payments, to pay bills, every parameter is different.

The Arbiter explains that parameters for payment by card are less than €3,000 and that is why it was refused, but the parameters for payment online transfers are as high as €25,000, for example, because at the last sitting when the Arbiter asked whether any of the payments made online necessitated an increase in limit, the reply was that, no, there was no need to increase the limit because since she was a premier customer, all the payments were within that limit. So, there is a big difference between payments made by card and payments made online.

It is being said that on the same day, 28 June 2023, there were six transactions which were declined according to the table exhibited by the bank. Asked to confirm that this was abnormal behaviour by the customer in view of the fact that the previous transactions had no issues of payments going through, I say that the customer tried to put €3,000 which was not allowed and, subsequently, she tried €2,500[47] *which was allowed and she kept on trying to transfer money but this was from her account to her account within the parameters of her card account, so there was no irregular behaviour as it was from her account to her account.*

Being asked the fact that the customer tried to carry out this transaction six times in a row was not flagged as abnormal behaviour, I say, no, because it was from her account to her account.

It is being said that, for this reason, I can also confirm that no bank representative ever contacted the client to question why she was trying to make these repeated attempts, I say that she did not subscribe to this service. I say, I wouldn't know.

[47] Probably should have said €1,500

But that would not have triggered an alert because it was to her own account.

Asked had she been subscribed to receive notifications from the bank would she have been contacted at that point, I reply that I wouldn't be able to say how the system works.

Asked whether I could confirm that there is no check or measure or a safeguarding system which would automatically flag these repeated transactions, I say, no; they would not flag. I do not think it would flag.

I say that the bank would have systems whereby any irregular behaviour is recorded but since it was a secure transfer from a customer's account to another bank account, the system deems it that the customer knows what is going on; the customer has the intention to do it and it is not irregular behaviour. We cannot have a banking industry whereby payments are stopped from one's bank account to the same person's bank account.

It is being said that the problem is that there were six repeated attempts in a span of a couple of hours. I say that this is not irregular behaviour because first she tried €3,000 which was beyond the limit and she kept on trying to find the right amount to transfer.

Asked to also confirm that the bank therefore never enquired as to the reasons why the card holder needed to do these transfers, I say no, not that I know of.

Asked to confirm that due to the difference in parameters, there was nothing effectively stopping or checking on irregular behaviour of the customer, I say that if the huge amounts had been transferred to a third-party IBAN, then the system would have triggerred it but since it was to her own IBAN with Revolut, then the system would not trigger.

The system did not trigger anything because the bank feels that the fact that it is being transferred to an own account with another bank does not justify their intervention.

Asked to confirm that the complainant never went to a branch to alter the parameters, I say that I checked whether she called the Call Centre because

usually people call the Call Centre to alter parameters. And I confirm that with regard to her card transfer, she did not alter the parameters. She was given the parameters when she had applied for the Premier card. When she applied for her Premier status with HSBC, she was advised on her parameters because Premier card holder have different parameters than Advanced card holders and the normal customers.

Asked whether it would be correct to understand that the threshold for a customer to be considered as a Premier customer would be an annual income of €70,000, I say that there are different criteria to be considered as Premier. It could be with regard to a certain home loan, eligibility of joint customers or an eligibility of a single customer.

Asked whether there are any income requirements, I say, yes. Asked what are those requirements, I say that, if I am not mistaken, for a single account holder, it is an annual income of €50K plus.

It is being said that despite the threshold for becoming a Premier customer is an annual income of €50K plus, there were no limits enforced on the daily parameters of SEPA payments.

I say that there are limits for SEPA transfers and customers are usually advised when they are upgraded to Premier.

The limit was more than €24K because the last payment was for €24K. So, €24K was within the limit.

Asked whether this was a high parameter for all Premier customers so whether the customer was in the range of an annual income of €50K or of €3M, it is the same parameter, I say that customers can opt to reduce the parameters. For instance, I can confirm on oath that when I had taken out my card system a few years back, maybe about twelve years ago, I set the parameter for €500 for my own safety. You are advised and you can advise through internet banking to reduce the parameters.

It is being said that the question is that internally the bank does not take any measures to cater for different parameters for different types of customers even at Premier level.

I say, no, there are different parameters at Premier level between Premier customers and other Premier customers.

Being asked since there are different parameters at Premier level, then how does the bank justify that it allows transfers of an amount equivalent to over half of the annual income threshold needed to become a Premier customer, I say that there is a default which applies to everybody but then, the bank, through the Relationship Manager, detects that certain customers need higher limits and the bank will provide the higher limits.

I say that the €25K is the default limit for all Premier customers.

I am being referred to my testimony where I presented a generic email sent to the bank's customers which addresses unauthorised use of credentials and security details.

Asked whether I am in agreement that this email does not address in any way authorised push payment fraud, I say that this email says, 'We'd just like to remind you to always be vigilant and ignore anything that seems suspicious or too good to be true. Always remember that we will never ask you to reveal your passwords.' (page 135)

We would never be able to cover all types of fraud immediately in one email, in one letter, but it is always good to be vigilant. It is general to all fraud.

Asked whether, apart from SMS alerts which the customer opts to receive to confirm payments which have been made, there are other types of SMS alerts to warn clients about suspicious fraud attempts, I say, no. The system works like this:

If [the Complainant] would have paid Mr Y in Hong Kong, with whom she had never done business with, a sum of €25K through SEPA, there is a high probability that she would have received a call (and not an SMS) because our monitoring system would have been triggered and the payment would have been suspended from going forward.

But in this case, it was from HSBC to Revolut.

It is being said that [the Complainant] had contacted the bank to inform them that she was a victim of this fraud.

Asked to confirm that no further action was taken from the bank vis-à-vis [the Complainant], I say that the bank told [the Complainant] to go to the Police Station to file a police report.

It is being said that recently on the HSBC App, when there are SEPA payments to be made, the bank is requesting a reason for those SEPA payments where there is a drop-down menu for the customer to input the reason why the request for the SEPA payment is being made.

Asked to confirm that this was not the case at the time when these transactions were happening, I say, no, I can't confirm because I remember a few years ago that I also had to put in the confirmation code. I can remember it clearly.

Asked again the above question, I say that, to my knowledge, this does not appear as something new. I can ask someone to confirm whether it is something new or not but I cannot confirm that this is something new. If it were something new, I would say that it is something new."[48]

In their final submissions,[49] the parties reiterated, in essence, the submissions previously made in the Complaint, reply and respective testimonies during the indicated sittings.

Analysis and Considerations

The Complaint, in essence, relates to the allegation that HSBC failed to have adequate controls in place to protect the Complainant from falling victim to an investment scam. She claimed that the Bank's systems failed to prevent her from falling victim to serious fraud as there were no warnings or interventions on the Bank's part that would have helped her realise that she was falling victim to a scam.

[48] P. 163 - 168
[49] P. 173 - 185 & P. 189 - 194

She claimed that the Bank failed to monitor and question the alleged abnormal transactions she had made on her account, with the result that she ended up losing much of her savings.

This case is one of the first in a series of cases filed by Maltese residents before the Arbiter regarding **fraudulent payment schemes** which have features of a scam known as **'pig butchering'**. Professional fraudsters with enormous creativity are using such techniques and methods to enrich themselves, particularly at the expense of vulnerable people.

Along with this decision, the Arbiter is publishing Technical Notes on what **'pig butchering'** is, explaining the obligations that banks and other licensed financial institutions have to protect clients, especially vulnerable ones, from this type of fraud. This is so that banks and licensed financial institutions adhere to their obligations and understand the consequences if they fail to do so.

These Technical Notes are also being published on the OAFS's website for general information, not just for the parties in this complaint.

The main aspect relating to the merits of this Complaint is whether the Bank acted according to its obligations regarding the monitoring of payments made by its client.

In the Technical Notes that the Arbiter has already issued regarding fraudulent payments,[50] it has already been declared as follows:

> *'PSPs are obliged to have effective monitoring systems of payments to protect their PSUs from payments frauds. Commission Delegated regulation (EU) 2018/389 of 27 November 2017 establishes regulatory technical standards for strong customer authentication and common and secure open standards of communication supplementing Directive (EU) 2015/2366.*
>
> *It states in article 2(1) that:*
>
> ***"Payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorized and fraudulent payment transactions … those mechanisms shall be based on the analyses of payment transactions taking***

[50] The Technical Notes issued in December 2023 (Updated Nov 2024) titled *'A model for allocation of responsibility between Payment Service Provider (PSP) and Payment Services User (PSU) in case of payment fraud scams'* - https://www.financialarbiter.org.mt/content/technical-notes

into account elements which are typical of the payment service in the circumstances of a normal use of the personalised security credentials."

Article 2(2) states that the following risk-based factors have to be included in the transaction monitoring mechanisms:

- *Lists of compromised or stolen authentication elements;*
- *The amount of each payment transaction;*
- *Known fraud scenarios in the provision of payment services;*
- *Signs of malware infection in any sessions of the authentication procedures;*
- *In case the access device or the software is provided by the payment service provider, a log of the use of the access or the software provided to the payment service user and the abnormal use of the access device or the software.*

It was clarified that the obligation for monitoring payments mechanisms need not be 'real time risk monitoring' and is usually carried out 'after' the execution of the payment transaction. How much after has not been defined but obviously for any real value of such mechanisms the space between real time payment and effective monitoring must not be long after.

Further article 68(2) of PSD2 authorises a PSP to block payments:

"If agreed in the framework contract, the payment service provider may reserve the right to block the payment instrument for objectively justified reasons relating to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument or, in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil its liability to pay."'

It is clear that there are serious obligations on a bank, like HSBC, to properly monitor the payments that its clients are making and to be attentive to any serious indication that the payments, although being authorised by the client, may contain suspicion of fraud where the client ends up a victim of professional fraudsters.

It is equally clear that the monitoring obligations go much further than checking individual payments. Consideration also must be given to a series of payments being made in the context of the normal payment history of the client concerned.

To assist in reaching an opinion on the effectiveness of the payment monitoring system adopted by the institutions, the Arbiter shall take various criteria into consideration as outlined in Table C below.

Table C

Criteria considered in the determination of whether the payments in question were abnormal and 'out-of-character' in the context of the Complainant's profile and her typical transactions

Basic criteria		**Particular information emerging from the case**
(a) Consumer profile		The complainant, who was 34/35 years old when the payments occurred, was described as a *XXX*' at an insurance company with a salary that varied between €5,700 and €9,000 per month.[51]
(b) **Amount and size of the transaction** (as compared to the average transaction amount and total account balance and/or monthly net income/revenue)		As it emerges from Table A, four of the payments complained of exceeded €5,000, with the last two payments being substantial and between them amounting to €42,000, which is 60% of all the payments complained of.[52] These were not at all typical of normal payments made from her accounts.
(c) **Frequency, timing and pattern** of the same or similar transactions		The ten disputed payments were made in quick succession within a week and a half, the first six (for the total of €15,100)[53] within two days, and the second three (for the total of €31,000)[54] within three days whilst another single substantial payment (of €24,000) after four days. Since the Complainant was a Premier client, she did not need to call to obtain specific authorisation for these

[51] P. 77 & 78
[52] Eur42,000 (18,000+24,000) of Eur70,100
[53] 700+8400+1500x4 = 15,100
[54] 5000+8000+18000 = 31,100

		payments because Premier clients had a sufficiently high payment limit for these payments to go through.
(d) **Cumulative amount** resulting from the same or similar transactions (as compared to the average transaction amount and total account balance)		In the space of eleven days (that is, between 30 June and 11 July 2023), the cumulative amount of payments made by the Complainant reached more than €70,000 which was the greater part of the available balance on her account. This amount was an average of around 9 months of the Complainant's normal net salary.
(e) **Scope of the transaction**		The purpose of the payments was to transfer money to the account she had with Revolut to make the various payments she was being requested. From there, this money was ultimately transferred to a fraudster, but HSBC could not have known about this unless contact was made with the client. The scope of the transactions, that is, to settle a series of payments she was being requested to make for the release of substantial profits she was led to believe were made over a very short period of time. This would likely have transpired if timely contact was made with the client.
(f) **Recipient of the transaction**		This was the Complainant's personal account held with Revolut. The ultimate beneficiaries were other parties – that is, the scammers.
(g) Any **relevant material public warnings on the recipient**		Revolut is a licensed bank and there was no justifiable reason for one to suspect of fraud in case of normal transactions. To note that the initial payment to trade was done on a platform - *'easycrypto4ucom'* - which even included clear reference to crypto in its name. Certain warnings on such platform already existed

		at the time.[55] The amount transferred to this platform of €250 was however relatively insignificant and would have reasonably and justifiably not triggered any intervention.
(h) Other **inconsistent or exceptional nature of the transaction or series of transactions** as compared to the historical operation of the account		There was a strong anomaly because the Complainant's accounts never had a history of such large and frequent payments in a short period of time. The only payments of substance, other than those complained of or shown in the complaint, were transfers between her own accounts with HSBC.

Although the criteria mentioned above are reflected in a structured manner in the Technical Note that the Arbiter is issuing with this decision, these criteria are not some new or onerous aspects that a bank takes, or should have taken, to adequately fulfil its obligation to monitor a client's transactions.

The bank already has information on most of these criteria in its systems, and others can be collected when intervention is timely and necessary as part of the bank's monitoring obligations.

It is the Arbiter's view that the disputed payments were anomalous compared to the Complainant's account history as presented during the case.[56] This was not contradicted by the Service Provider.

Therefore, the Bank should have intervened at some point during these payments to have a serious conversation with the Complainant to understand what was happening with her account and assess the possibility of fraud.

The Bank has, or should have, enough experience to be aware of how professional and increasingly creative fraudsters are leaving a trail of victims through false promises of easy and quick profits.

[55] https://www.cybercrimepolice.ch/de/warnung/verdaechtige-online-plattformen/easycrypto4ucom/

[56] P. 67 - 100

It is acknowledged that the point at which the Bank should have had enough suspicion to discuss potential fraud with the Complainant is a subjective argument.

The Arbiter believes it is fair to conclude that this point should have been reached by July 6, 2023, after these payments were already made:

TABLE D

DATE	*MASTERCARD CARD EURO*	*SEPA OnLine Euro*	*Account from where payment was made*
30.06.2023	700		IBAN … 82
30.06.2023		8400	JOINT SAVINGS
30.06.2023		1500	JOINT CURRENT
30.06.2023		1500	SAVINGS …50
01.07.2023		1500	JOINT CURRENT
01.07.2023		1500	SAVINGS …50
05.07.2023		5000	SAVINGS …52
06.07.2023		8000	SAVINGS …52

The above had already generated a series of transactions not typical of the Complainant amounting in total to €28,100 within less than a week, this being already a high portion of her savings. Additional substantial payments (of €18,000 and €24,000), as was shortly attempted and made thereafter by the Complainant within just one to five days, on 7 and 11 July 2023 should have triggered the Bank's intervention irrespective of the relatively high withdrawal limits applicable on the account of €25,000.

This takes also into consideration that, at the same time, there was some strange anomolous activity where the Complainant attempted to make many payments that were largely rejected because they were outside the parameters of the card account (see Table B above).

For this purpose, the Arbiter is exempting HSBC from all liability regarding the first payments that were made up to July 6, 2023. This also takes into consideration the fact that the Complainant had received an email notification from the Bank to be careful of scammers and fraudsters who, to deceive, promise things *'too good to be true'*.[57]

However, the Arbiter also feels that important notices like these deserve specific direct communication and not as part of a communication involving many topics spread over several pages, which easily loses its effect on the recipient. This is apart from the fact that the diluted warning related more to the authorised access to one's account rather than online investment scams.

From this point of 6 July 2023 onwards, there is accordingly a strong argument that the Bank failed in its duties under the obligations of payment handling according to PSD 2 and, therefore, must bear a portion of the loss that the Complainant suffered regarding the other payments after that point, that is:

TABLE E

DATE	***MASTERCARD CARD EURO***	***SEPA OnLine Euro***	***Account from where payment was made***
07.07.2023		18000	SAVINGS …52
11.07.2023		24000	SAVINGS …52
TOTAL		42000	

Final Observations

Whilst it is neither expected nor should it be that a bank intervenes in every payment there is, however, there are reasonable and justifiable particular circumstances where a bank has the obligation and duty to intervene. This is

[57] P. 135

particularly so, for example, when there is an abnormal material payment or a series of transaction which are anomalous.

The Bank's defense for not bearing any responsibility is based on the argument made that since the payments were in favour of the Complainant herself into her Revolut account, and there was no involvement of third parties, then, the Bank had no obligation to question what the Complainant was doing with her money.

This defense holds up to a certain point but then falls apart. This point was until **July 6, 2023**. At that time, the Bank should have had clear signs from the payment monitoring system that something very strange was happening with the Complainant's behaviour. The Complainant was passing all these payments in a very short amount of time, even though they were going into her own account with Revolut.

The Bank knew that the Complainant had never made these types of transactions **with such a concentration of time and value**. Therefore, when the Complainant came to make the last two payments for much larger amounts than before, with the history of payments already made in the days before, the Bank had a duty to stop those payments due to clear red flags about the operation of her account and open a serious conversation with the Complainant.

Another argument that mitigates HSBC's guilt is that the Complainant was an educated person, a graduate, working in XXXXX in insurance, who had a substantial salary that testified to the position of responsibility she held and, therefore, it was argued that she was not a person that one would think would fall for the bait of fraudsters.

The Arbiter understands this argument and, therefore, feels that the Complainant should also bear a reasonable portion of the loss, even from the last two payments, apart from the entire burden of the previous payments. It is to be pointed out, however, that the level of sophistication of scams has increased substantially over the past years, and even highly educated and professional people are also falling victims of sophisticated scams as also seen by the Arbiter from his experience.

There are also studies suggesting that well-educated persons are far from being much less vulnerable than some may think.[58]

Whilst the Bank was reasonably not expected to undertake any *due diligence* on the integrity of the parties that the Complainant was dealing with, and neither was it expected to give advice to the Complainant unless so requested, it is, however, reasonable and legitimate to expect the Bank to have intervened as outlined above. There were sufficient reasons where the Bank could have:

i. blocked and suspended the payment of 7 July 2023 and verified the reasons why the Complainant was making multiple successive material payments from her accounts which were not reflective of her typical transactions;

ii. verified with the Complainant the nature of the payments, their scope and to whom these were effectively being paid;

iii. given the evident high-risk nature of the payments escalated its investigations asking simple basic questions and drawing the Complainant's attention to certain aspects and *'red flags'* that emerged. Possible questions or aspects raised with the Complainant could, for example, have included the following:

- how she got to know about the trader (which would have transpired from social media);
- whether she had ever met the trader personally and whether she has verified that the trader with whom she was dealing with was truly who he was claiming to be and regulated by a reputable financial services authority in respect of the services offered;
- whether she had ever done such type of transactions before;
- the extent of claimed profits made and over which period (which sounded too good to be true) and the reasons for the payment

58 https://ijssrr.com/journal/article/download/1840/1427/#:~:text=Those%20with%20a%20higher%20college,become%20victims%20of%20investment%20scams.

demands being made despite the claimed profits which all had the typical features of a scam.

Such aspects would have continued to heighten the *red flags* about her transactions and the probability of a *scam* given also the extent of pressure made by the scammers in demanding payments. In such circumstances, the Bank could have further drawn the client's attention:

- about the various types of sophisticated fraudulent schemes that involved the type of transactions that the Complainant was doing or attempting to do and the need for her to be careful and thoroughly verify her situation not to fall a victim of a scam;
- encourage one to exercise caution and seek professional assistance such as from someone licensed locally who can guide her accordingly given the emerging red flags in her particular case.

The Arbiter does not share the Bank's view that:

> *'Any prior warning that may have been provided by the Bank to prompt her about the beneficiary of the payment would not have prevented Complainant from declining to credit her own account with a third-party payment service provider,'*

as claimed in its reply of 16 May 2024.[59]

The Complainant had a long-standing relationship with the Bank, having been a Premier Customer of the Bank since 2020. HSBC was also her primary bank with whom she had a mortgage and, also, received her salary.

The Complainant had initially exercised certain caution by starting with a low investment amount of EUR250 and doing certain checks on the providers (like checking the FCA's register), which were not sufficient and adequate given the extent of the deceit and sophistication of the scammers.

The Complainant was indeed later suspicious at various points. For example, in her email of 27 June 2023, she noted,

[59] P. 107

> *'Have no words to be honest, **if this is real**, hats off to you … will let you know once received …'*.[60]

In her email of 29 June 2023, the Complainant stated:

***'What guarantee I have that they will not request further money now? …** I noticed the wallet address is different now, and the money needs to be sent in USD and BTC right? ... I would not like to transfer more money to be honest …'*.[61]

She also questioned other aspects, like the request for insurance payment as per her email of 29 June 2023,[62] and did general searches on other parties like Binance and Trust Wallet but did not realise she was dealing with impersonators and fake parties until she probed in detail the scammer's latest request for tax payment at which point she confirmed her fears about the scam.

A timely warning from the Bank, where the Bank would have added its suspicion on top of those already held by the client, and encouragement to carefully verify things and exercise great caution given the red flags and features of a typical scam, would have been helpful in the circumstances as it would have aided in stopping the scam in its tracks.

The Arbiter would like to finally observe that Article 19(3) of the Act relating to the functions and powers of the Arbiter, provides that:

> *'(3) In carrying out his functions under sub-article (1), the Arbiter shall:*
>
> *…*
>
> *(c) consider and have due regard, in such manner and to such an extent as he deems appropriate, to applicable and relevant laws, rules and regulations, in particular those governing the conduct of a service provider, including guidelines issued by national and European Union supervisory authorities, good industry practice and reasonable and legitimate expectations of consumers and this with reference to the time when it is alleged that the facts giving rise to the complaints occurred; …'*

[60] P. 41 – Emphasis added by Arbiter
[61] P. 48 – Emphasis added by Arbiter
[62] P. 47

This decision and the Technical Note attached to it already treat the regulatory aspect. As to the good industry practice followed in financial areas, the Arbiter further observes that the concept and expectation that a bank adequately intervenes in anomalous and out-of-character transactions is far from a new concept. Although the practice is not necessarily the same in every jurisdiction, the Arbiter considers that one cannot ignore the practice of banks, for example, in reputable jurisdictions in the financial sector such as that of the United Kingdom, which places the protection of the consumer's interest first, and where even HSBC has its headquarters. There are, for example, a good number of decisions from the UK Financial Ombudsman (FSO) on this aspect that go back to 2022.[63] A common aspect that emerges from such decisions in fact, is that:

> '*There are circumstances in which a bank should make additional checks before processing a payment, or in some cases, decline to make a payment altogether, to help protect its customers from the possibility of financial harm.'*

In cases of fraud-scams complaints, FSO generally protects consumers where a UK financial institution allows payments by an unexperienced investor directly to a crypto exchange.

> *'We thought the spending on Marta's account was very unusual for her and – after the first few payments – the pattern of transfers from her account should have caused the bank some concern meaning that it ought to have intervened. We thought that if the bank had asked Marta about the transactions she would have told it what she was doing. Even though the payments went to a crypto account in her own name, we felt that the bank was sufficiently aware of the common features of this kind of scam and should have warned about the risk of being scammed and the need for her to make further enquires at this point.*

[63] Cases 'DRN-3563742', 'DRN-3670635' and 'DRN-4549050' against *HSBC UK Bank plc* decided by the UK Financial Ombudsman in 2022, 2023 and 2024 respectively -
https://www.financial-ombudsman.org.uk/decision/DRN-3563742.pdf
https://www.financial-ombudsman.org.uk/decision/DRN-3670635.pdf
https://www.financial-ombudsman.org.uk/decision/DRN-4549050.pdf

As Marta's circumstances had many of the hallmarks of a cryptocurrency scam and taking into account what we learnt about Marta through the course of the complaint, we thought a conversation would have made a difference and would, more likely than not, have prevented further loss.

In deciding fair compensation, we also considered if would be fair for Marta to bear any additional responsibility for what happened. However, as we thought the trading platform and correspondence with the fraudsters was very convincing, we decided against that on the facts of this case. So, we asked the bank to refund all the transactions which took place after the point we thought it should have intervened.' [64] [65]

The Arbiter also recognises and takes into account the reasonable and legitimate expectations of the consumer as also required by law. The Complainant ultimately expected her Bank to take certain measures to protect her from fraudulent transactions.

In this context, the Arbiter considers that the Bank did not meet the obligations mentioned and the legitimate expectations of the Complainant and it is just, fair and reasonable for the Complainant to receive an element of compensation due to the identified shortfalls on the Bank's part.

There is also no doubt that certain material shortcomings emerge on the part of the Complainant and the Arbiter will consider all these aspects in the extent of compensation awarded.

[64] https://www.financial-ombudsman.org.uk/decisions-case-studies/case-studies/consumer-contacts-us-complain-cryptocurrency-investment-scam

[65] The Arbiter is not applying 100% recovery as in the FSO case referred to given *inter alia* the payments were not made directly to a Crypto platform.

Decision

For the reasons amply explained above, the Arbiter decides that HSBC failed in its obligations of payment monitoring in respect of certain transactions undertaken by the Complainant.

If the bank had engaged in a proper conversation with the Complainant at some point before the last two payments, which were for a much larger amount than the previous ones, it would have explained that the payments she made and intended to continue making had a clear indication of fraud and could have dissuaded her from making further payments.

The Arbiter, therefore, orders HSBC to refund part of the loss suffered by the Complainant due to its material shortfall in the payment monitoring system and pay the Complainant forty per cent of the last two payments, that is, 40%[66] of €42,000, which amounts to €16,800 (sixteen thousand and eight hundred Euro) in terms of Article 26(3)(c)(iv) of CAP. 555.

With interest at the rate of 3.15% p.a.[67] payable within five days from the date of this decision until the date of effective payment.[68]

Each party is to bear its own costs of these proceedings.

The Arbiter is also ordering HSBC to carefully understand the conclusions of the Technical Note annexed to this decision and make sure that the right investments are in place for the systems and training of its staff for the effectiveness and robustness of its payments monitoring and to safeguard the interests of its clients from the relentless and cruel hunt by increasingly professional and creative fraudsters.

The Arbiter also opines that in a scenario of alarming increase (locally and internationally) of fraud-scam schemes, banks should apply lower default daily transaction limits and let customer take the initiative to increase such limit if they so wish, rather than set high default daily limit and inform customers in

[66] In decisions about similar complaints being issued concurrently, compensation was set at 50%. In this case, the Arbiter is setting a lower recovery rate to take into account the 'status' of the Complainant as a XXXXX.
[67] Equivalent to the current Main Refinancing Operations (MRO) interest rate set by the European Central Bank.
[68] It is to be noted that in case this decision is appealed, should this decision be confirmed on appeal, the interest is to be calculated from the date of this decision.

their terms and conditions that they can opt to reduce them. Opting to increase the daily limit would permit the bank to inform customers of the risks involved in adopting high limits.

Alfred Mifsud
Arbiter for Financial Services

Information Note related to the Arbiter's decision

Right of Appeal

The Arbiter's Decision is legally binding on the parties, subject only to the right of an appeal regulated by article 27 of the Arbiter for Financial Services Act (Cap. 555) ('the Act') to the Court of Appeal (Inferior Jurisdiction), not later than twenty (20) days from the date of notification of the Decision or, in the event of a request for clarification or correction of the Decision requested in terms of article 26(4) of the Act, from the date of notification of such interpretation or clarification or correction as provided for under article 27(3) of the Act.

Any requests for clarification of the award or requests to correct any errors in computation or clerical or typographical or similar errors requested in terms of article 26(4) of the Act, are to be filed with the Arbiter, with a copy to the other party, within fifteen (15) days from notification of the Decision in terms of the said article.

In accordance with established practice, the Arbiter's Decision will be uploaded on the OAFS website on expiration of the period for appeal. Personal details of the Complainant(s) will be anonymised in terms of article 11(1)(f) of the Act.

Technical Note

Guidance on considerations that the Arbiter will adopt in determining complaints related to *'pig butchering'* type of scams

A) Background

Following the model issued by the Arbiter in December 2023 regarding the allocation of responsibility between a Payment Service Provider ('PSP') and a Payment Service User ('PSU') in case of payment fraud scams, the Arbiter now considers it timely to similarly issue general guidance about the considerations relevant to complaints involving other emerging sophisticated scams, like those commonly known as ***'Pig Butchering'*** scams.[1]

Scammers are continually evolving their schemes to defraud innocent and vulnerable financial consumers of their hard-earned savings. ***'Pig Butchering'*** is one of the evolving and serious fraudulent schemes that have escalated rapidly in recent years. It often causes grave consequences to the victim beyond the direct impact of significant financial loss. Besides the devastating financial consequences, it can have grave emotional consequences, including one's self-confidence and self-respect, possibly leading to tragic conclusions.

Having seen a rise in complaints involving such scams, the Arbiter is issuing this Technical Note to increase awareness and outline the considerations that will shape the Arbiter's decisions. The aim is to ensure fairness, consistency, transparency and objectivity to the complaint's process for all parties involved. Service Providers are hence encouraged to review and adopt this Technical Note.

The considerations outlined in this Technical Note are for guidance purposes only. The merits of a complaint will continue to be assessed and determined on a case-by-case basis with the particular circumstances of each case considered accordingly.

[1] *Interpol has recently suggested substituting the term 'Pig Butchering' with something more respectful to victims. (https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-urges-end-to-Pig-Butchering-term-cites-harm-to-online-victims). As no new term has yet gained international recognition, OAFS is temporarily continuing to use the term **'Pig Butchering'** to ensure that potential new victims know what we are referring to and are deterred from falling into the fraud trap. For the future, we plan to use the term 'Relationship Confidence Fraud' or similar.*

If the specific circumstances so necessitate, the Arbiter may depart from certain aspects outlined in this Technical Note or take into account and/or attribute greater importance to one or more aspects as considered appropriate. The reasons for the position taken will be duly outlined, in writing, in the Arbiter's decision with each case determined and adjudicated by reference to what, in the Arbiter's opinion, is fair, equitable and reasonable in the particular circumstances and substantive merits of the respective case.[2]

B) What is *'Pig Butchering'*

***'Pig Butchering'* is a scam where the scammer may use a variety of methods, such as social engineering and psychological manipulation, to establish a relationship** (either social, romantic, or business focus), **gain the victim's confidence and trust** and then, **gradually and deceivingly, introduce the victim to a fraudulent investment opportunity** with the fraud typically carried out **over an extended period**, often lasting several weeks to months.[3]

In most cases, scammers **first approach victims through social media or dating apps** and may ask to take the conversation to a different platform (e.g. WhatsApp, WeChat, Telegram or other messaging app). Potential victims **might also be approached directly on messaging apps**. The **scammer would communicate regularly with the victim** with the aim **to establish and maintain a relationship**.

Once the scammer **gains the victim's trust and attention** the scammer will propose an investment opportunity, typically involving crypto-assets (but may involve other assets). The scammer will offer to train the victim to set up an account on an exchange to purchase crypto-assets, and then provide a wallet address for the victim to transfer funds in order to participate in the investment opportunity. Examples of such investment opportunities might involve:

- the offer to trade online in well-known crypto-assets (or other assets) where victims are directed to fake or cloned trading platforms that would show fictitious trading and false returns;

[2] CAP. 555, Art. 19(3)(b)

[3] In the Annex to this Technical Note, there is a brief summary of typical scenarios used by scammers in pig butchering scams and other scams.

- investment in new crypto-assets or tokens;
- high-yield investment opportunities or other investments promising high-profit levels over a short period of time.

The **fraudulent investment opportunity is designed to appear legitimate** and often **produces artificial significant gains** to keep the victim engaged and lured to deposit even more funds. **Scammers exploits psychological factors, such as the fear of missing out, to manipulate victims into starting and continuing investing**. Scammers often adopt false identity and impersonification to give the impression that they are a professional person or related to respectable licensed institutions when this is not the case.

The victim is eventually never able to withdraw funds and the fictitious profits. **In the final stages of the scam, the victim is typically asked to transfer even more funds before anything can be withdrawn** through a variety of excuses for such payment requests (e.g. service fees, taxes, etc.). A **sense of urgency** is often created at that stage **for the victim to immediately settle payment requests** with the excuse that otherwise high penalties would be incurred, their account blocked or frozen or their funds completely forfeited. These would, however, be just further **attempts to continue extracting more money from their victims**.

This type of **scam ultimately causes the victim to suffer significant financial loss**, often resulting in the **loss of a substantial portion, if not all, of their savings or even accumulation of debt**.

C) How is *'Pig Butchering'* different from APP scams?

It is different and probably more cruel than a phishing or smishing payment fraud or Authorised Push Payment ('APP') fraud schemes, about which the Arbiter has already issued Technical Notes on how the responsibility for the loss is to be allocated between the consumer victim and the Payment Service Provider (the PSP being the bank or financial institution making the payment).

Whereas, for example, an APP fraud is often a one-shot transaction for an amount not exceeding the daily payment limit agreed with the PSP, ***'Pig Butchering'* fraud often involves a series of transactions over a span of time** and, accordingly, generally involves much larger losses.

Given that such scam happens over a period of time (sometimes several weeks or months) and involves a series of transactions, victims who have approached the Office of the Arbiter for Financial Services ('OAFS') in recent cases filed complaints *inter alia* against banks claiming fault by their service provider for not intervening and alerting them to the scam as part of the service provider's payment transaction monitoring obligations.

D) Payment transaction monitoring obligations

There are different types of licensed service providers that are particularly affected by these types of scams.

Such service providers can be divided into three different broad categories:

a. Banks/Credit Institutions licensed under the Banking Act[4]

b. Financial Institutions, including Payment Institutions, licensed under the Financial Institutions Act[5]

c. Virtual Financial Assets Service Providers licensed under the Virtual Financial Assets Act.[6]

The operating licences of the said providers impose on them different levels of obligations related to payment transaction monitoring. However, licensed service providers are subject to overall fiduciary duties to their clients in terms of the Civil Code and their license conditions.

(i) **<u>Banks and Credit Institutions</u>** are considered to have a very high level of obligations for transaction monitoring to protect their clients from fraud schemes. This is also a result of the general long-term relationship between the Bank and its clients, permitting the Bank to build a reliable picture of the normal transactions that clients pass through their account. Financial Institutions and Virtual Asset Service providers may not necessarily enjoy such long-term relationships with their clients.

[4] CAP. 371
[5] CAP. 376
[6] CAP. 590

Banks and credit institutions are obliged to have effective monitoring systems of payments to protect their PSUs from payment fraud.

For example, Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 establishes regulatory technical standards for strong customer authentication and common and secure open standards of communication supplementing Directive (EU) 2015/2366.[7] It states in article 2(1) that:

> "***Payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorized or fraudulent payment transactions …***
>
> ***Those mechanisms shall be based on the analysis of payment transactions taking into account elements which are typical of the payment service user in the circumstances of a normal use of the personalised security credentials.***"

Article 2(2) of the said Commission Delegated Regulation furthermore states that:

> ***"Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:***
>
> ***(a) lists of compromised or stolen authentication elements;***
>
> ***(b) the amount of each payment transaction;***
>
> ***(c) known fraud scenarios in the provision of payment services;***
>
> ***(d) signs of malware infection in any sessions of the authentication procedure;***
>
> ***(e) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software."***

[7] https://eur-lex.europa.eu/legal-content/EN-MT/TXT/?from=EN&uri=CELEX%3A32018R0389

It was clarified that the obligation for monitoring payments mechanisms need not be *'real time risk monitoring'* and is usually carried out *'after'* the execution of the payment transaction.[8] How much after has not been defined but obviously for any real value of such mechanisms the space between real-time payment and effective monitoring must not be long after.

Article 68(2) of PSD2 also authorises a PSP to block payments:

> "***If agreed in the framework contract, the payment service provider may reserve the right to block the payment instrument for objectively justified reasons relating to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument or, in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil its liability to pay.***"

Anti-money laundering legislation further provides other legal basis for monitoring transactions and the freezing or blocking of accounts in case of *inter alia* suspicion of fraudulent activities.

(ii) **<u>Financial Institutions, including Payment Institutions, licensed under the Financial Institutions Act</u>**

The provisions referred to earlier similarly apply to payment service providers licensed under the Financial Institutions Act. Claims received from personal customers against such institutions were often based on the expectations that payments made to third-party beneficiaries indicated by the fraudsters, were made to accounts that such third parties held with the financial institution concerned. Victims, therefore, claimed recoveries from the financial institution concerned for failing to stop payments or for offering account facilities to beneficiaries involved in the fraud scheme.

The merits of such claims generally depend on the pattern and size of payments involved. However, given that there might be no established history of account operations between the complainant and the PSP, it would be harder to prove fault on the PSP transaction monitoring system.

[8] https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2018_4090

Furthermore, such claims are often challenged by the PSP on the basis that the Arbiter does not have competence to hear and adjudicate them as the complainant (victim) is not their eligible customer as defined in the Arbiter for Financial Services Act, Chapter 555 of the Laws of Malta ('the Act').

Amendments to the Act are to bring such complainants within the definition of *'eligible customer'* so that the Arbiter would be able to adjudicate such claims on their particular merits. The merits could then include an **examination of the robustness of the service provider's procedures for the onboarding of B2B clients that are involved in or allow themselves to be exploited by fraud schemes.**

(iii) **<u>Virtual Financial Assets Service Providers</u>** – These include service providers offering services of custodial wallet and the purchase and sale of digital assets through the wallet. The services also involve the transfer of digital assets to, and from, other *digital* wallets both hosted and external.

In many of the cases received by the OAFS, the complaint related to an alleged fraudster who persuaded and actively assisted their victim to open a digital wallet account with the VFA service provider, transfer funds from their normal bank account to such wallet account, and then use the funds for the purchase of digital assets, like Bitcoin and USDT, amongst others.

These digital assets were subsequently typically then transferred by the victim, under the direction of the fraudster, to an unhosted external wallet, under the control of the fraudster where external wallets would not offer visibility of their ultimate beneficiaries. Assets received in such wallets are then transferred out by fraudsters through a complex web of transactions which make it difficult to trace their ultimate destination.

When victims ultimately realise that they have been scammed they raise a complaint against the VFA service provider claiming that the VFA provider failed to protect them from fraudsters and that they should have stopped the transfer of their assets to the external wallet. Such complaints typically invoke the obligations of the VFA for Anti-Money Laundering and Financing of Terrorism (AML/FT) obligations or referring to provisions of the Payment Services Directive which may not necessarily apply.

In most cases adjudicated so far, the Arbiter could not uphold the victims' claim as:

1. The Virtual Financial Assets Act ('VFA Act') does not provide for similar transaction monitoring obligations that banks have under Central Bank of Malta Directive No. 1 – The Provision and Use of Payment Services (Ref. CBM 01/2018) which states that "***This Directive is modelled on the requisites of the Directive (EU) 2015/2366***".[9]

2. AML/FT obligations are covered by Implementing Procedures issued by the Financial Intelligence Analysis Unit (FIAU) as applicable to the Virtual Financial Assets Sector.[10] However, any infringements to such Implementing Procedures fall under the prerogative and responsibility of the FIAU who may sanction the licensee as appropriate for its failure, but does not offer adjudication services in favour of the fraud victims.

Guidance going forward

(i) <u>Banks and Credit Institutions</u>

Banks are urged to ensure that substantial upgrades have been made to their payments monitoring systems. Banks have the benefit of long-term relationships with their clients, and they **need systems which are sensitive to new patterns compared to historical trends**. **New patterns should be flagged**, and **customer needs to be alerted and advised** accordingly. **Conversations with clients are to be properly recorded** so that they may serve as evidence in the adjudication process.

Banks should be aware of common features of scams and have an **obligation to warn their client about the risk flagged by abnormal deviation from their normal payments pattern** and the risk that this could involve a scam. **Further enquiries and an appropriate conversation with their customer could make a difference** and prevent augmentation of a fraud scam in its nascent stage.

[9] Directive-1.pdf (centralbankmalta.org)
[10] FIAU Part II (fiaumalta.org)

Banks' defence that changed pattern payments did not merit their intervention as they just involved transfer to customer's own account with a third-party bank or institution or VFA service provider are valid only up to a point.

Banks should have enough experience to raise doubts about certain crypto account operations by a retail client being untypical and raise suspicions. Untypical transfer/s should be looked upon with due suspicion even in case of me-to-me payments.

For an out-of-character transaction or once a pattern takes certain shape and amounts transferred start becoming frequent and accumulating being totally out of shape with past historical pattern of payments, Banks need to intervene to alert their customer before it gets too late.

At which point in a transaction or pattern banks should intervene to alert and have a conversation with their client depends on the circumstances of each case but doing nothing and relying on the me-to-me payments argument, will not find favour with the Arbiter.

When it comes to transaction monitoring obligations and assessment of appropriate action by the service provider, the Arbiter shall accordingly also take into consideration the following:

- **at which point/s the bank intervened**;
- the **extent and type of intervention**/s that was taken by the bank;
- the **behaviour and actions of the complainant following any such intervention/s**.

The Arbiter will particularly take into account the above with respect to unusual or out-of-character transactions. **The considerations that would be made to determine whether a transaction is considered unusual or out-of-character include *inter alia* any one or a combination of the following in the context of previous historical transactions and the customer's profile**:

(a) the **amount and size of the transaction** (as compared to the average transaction amount and total account balance and/or monthly net income/revenue);

(b) the **frequency, timing and pattern** of the same or similar transactions;

(c) the **cumulative amount** resulting from the same or similar transactions (as compared to the average transaction amount and total account balance);

(d) the **scope of the transaction**;

(e) the **recipient of the transaction**;

(f) any **relevant material public warnings on the recipient**;

(g) other **inconsistent or exceptional nature of the transaction or series of transactions** as compared to the historical operation of the account.

(ii) <u>Financial Institutions, including Payment Institutions, licensed under the Financial Institutions Act</u>

The provisions referred to earlier (in section (i) above for Banks and Credit Institutions), similarly apply to those payment service providers licensed under the Financial Institutions Act with whom the client has a payment account directly.

Financial institutions should be ready to defend complaints against them based on their merits and not rely entirely on the Arbiter's lack of competence to hear and adjudicate complaints against them on the basis of the complainant not being their eligible customer.

In particular, they should **adopt more robust onboarding procedures for corporate customers** that receive transfer of funds in their account from retail clients which carry the fingerprint of payments for investment services. Where their corporate clients receiving retail type funds happen to be involved in typical licensable activities, the financial institution needs to have **comfort that their corporate clients have proper onboarding systems for their own clients**. Furthermore, there must be **a convincing reason why corporate clients based in other jurisdictions involved in activities typically licensable sought account holding service with a Malta based financial institution**.

Where the fraud scheme involves a series of payments over a short period of time, the obligation for the institution to intervene at some point before continuing to process the payment, increases at each step of the way. Especially

when the payment order from the retail client gives only the IBAN number without clear identification of the beneficiary, the level of suspicion and need for investigation increases.

(iii) <u>Virtual Financial Assets Service Providers (VASPs)</u>

VASPs should be aware that with the coming into force of Regulation (EU) 2023/1113 and the Travel Rule Guidelines[11] their obligation to have reliable records on the owners of external (unhosted) wallets increases exponentially as from 30 December 2024.

Arguments that they have no means of knowing who are the owners of external wallets which have been whitelisted for payments by their client will lose their force.

VASPs have been long encouraged by the Office of the Arbiter (in decisions dating back from 2022),[12] for the devise of enhanced mechanisms to mitigate the occurrence of customers falling victims to such scams.

Furthermore, in the Arbiter's decisions of recent months there is a recommendation that VASPs should enhance their on-boarding processes where retail customers are concerned warning them that custodial wallets may be used by scammers promoting get-rich-quick schemes as a route to empty the bank accounts of retail customers and disappear such funds in the complex web of blockchain anonymous transactions.[13]

Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications.

VASPs are reminded that whilst their license under the VFA Act does not oblige them to adopt payments transactions monitoring mechanism as the PSD2 rules imposed on banks and credit institutions, Article 27(2) of the VFA Act obliges

[11] *Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113* - EBA/GL/2024/11 of 04/07/2024

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1113

https://www.eba.europa.eu/publications-and-media/press-releases/eba-issues-travel-rule-guidance-tackle-money-laundering-and-terrorist-financing-transfers-funds-and

[12] Such as Case ASF 158/2021
[13] Such as Case ASF 069/2024

them to the same fiduciary obligations as established in the Civil Code, in so far as they are applicable.

The lack of past long term relationship records does not readily offer them the possibility, as generally available to banks, to note patterns out of norm to their historical trends. But **if within the short-term span of transaction records, there are certain payments which are out of norm with the rest of the records, or if the transactions leading to the fraud are out of character with the KYC profile on the basis of which the customer was onboarded, the general fiduciary obligations should call for proper investigations and timely conversation with the client to warn against the possibility of fraud scams**.

For example, a payment for an amount which is evidently higher than other payments could be indicative of the fraudsters doubling down on their pig butchering attempts on the client (as was seen in cases where clients were demanded payment by the scammer equivalent to the supposedly accumulated profits for 'strict identification' excuses, with a fake promise to return the payment and profits).

Conclusion

It is in the interest of the industry to go the extra mile, even beyond regulatory requirements to ensure that consumers' confidence in the financial system is not eroded by the ease with which they perceive being tricked by fraudsters without proper protection from financial service providers.

The adjudication awards decided by the Arbiter will reflect the obligation of fairness, reasonableness and equity demanded by the Act through proceedings held informally and expeditiously but will also reflect the push that institutions need to invest in upgrading their monitoring systems in the interest of keeping a safe payments infrastructure.

The decisions on pig butchering fraud cases issued concurrently with these Technical Notes adopt a more lenient assessment of the transaction monitoring obligations of licensed institutions than would be adopted in future once the institutions have the benefit of considering, absorbing and adopting these Guidance Notes.

Consumers are also reminded to exercise caution, be careful in their dealings and stay aware of the specific risks associated with crypto-assets. In December 2024, the European Securities and Markets Authority (ESMA) issued additional warnings about crypto-assets, which consumers are urged to consider thoroughly.[14]

Consumers, especially retail type, should always bear in mind the maxim that if something is too good to be true, then, probably it is.

Issued: January 2025

[14] https://www.esma.europa.eu/sites/default/files/2024-12/ESMA35-1872330276-1971_Warning_on_crypto-assets.pdf

ANNEX

Summary of a few typical scenarios scammers use to trap victims in scams:[15]

Investment scams

Scammers use convincing marketing and new technology to make their investment sound too good to miss. They promise you big payouts with little or no risk. They often use pressure tactics to get you to act fast, so they can steal your money.

Jobs and employment scams

Scammers offer jobs that pay well with little effort. They pretend to be hiring on behalf of high-profile companies and online shopping platforms. Sometimes, the job they list does not even exist. Scammers also impersonate well-known recruitment agencies. Their goal is to steal your money and personal information. They may ask you to pay money upfront to be able to work for them.

Products and services scams

Scammers pose as buyers or sellers to steal your money. They set up fake websites or profiles on legitimate retailer sites offering products or services at prices that are too good to be true. They post fake ads and fake reviews. They may use stolen logos and domain names making such scams hard to spot. Scammers also pose as businesses that you know and trust to send you fake bills. They can even change details on legitimate invoices so that customers end up paying the scammer instead of you.

Romance scams

Scammers use the promise of love, dating, or friendship to get your money. They go to great lengths to convince you the relationship is real and manipulate you to give them money. Scammers find you on social media, dating or gaming apps and websites. They might also text or email you. They hide behind fake profiles and identities, sometimes of famous people.

[15] Source: https://www.scamwatch.gov.au

Once you trust them, they will have an ‘emergency’ and ask for your help. This will often be requests for money or other products.

Threats and extortion scams

Scammers pretend to be from a trusted organisation and claim you need to pay money or something bad will happen. They may threaten you with arrest, deportation, or even physical harm, if you do not agree to pay them immediately. They can also blackmail you by threatening to share naked pictures or videos you have sent them unless you send them money.

Unexpected money scams

Scammers try to convince you that you are owed or entitled to money or winnings that you did not expect to receive. The scammer asks you to pay a fee or to give your banking or identity details before you can collect the money or winnings. Unfortunately, there is no free money.