

Before the Arbiter for Financial Services

Case ASF 155/2024

PU

(the 'Complainant')

Vs

OpenPayd Financial Services Malta Limited

(C 75580)

('OPFS', 'OpenPayd' or 'Service Provider')

Sitting of 28 February 2025

The Arbiter,

Having considered in its entirety, the **Complaint** (filed on 7 August 2024), including attachments filed by the Complainant,¹

The Complaint

Where, in summary, the Complainant claims to have made three payments to an account number which was with OPFS for an amount of GBP £23,300 from her account with WISE in UK² in the following order:

16.11.2023 GBP 1,000

30.11.2023 GBP 18,800

12.12.2023 GBP 3,500

¹ Pages (p). 1 - 7 and attachments p. 8 - 75

² "... an electronic money services provider regulated by the Financial Conduct Authority (FCA) in the UK" - <https://wise.com/gb/blog/is-wise-a-bank-uk#:~:text=Wise%20is%20a%20UK%2Dbased,used%20all%20over%20the%20world.>

Complainant claims to have lost all this money as these transfers were instigated by fraudsters who were manipulating her vulnerability and, at age 72, she is now unable to afford to stay in her home. As the Complainant is a vulnerable person, and her health has been negatively affected by the ordeal of the fraud related to this Complaint, she was represented in the process by her daughter Mrs. "EE".

The Complainant maintains that there needs to be tighter security to help prevent vulnerable adults who are forced to try and survive in a world where they need to manage technology they simply do not understand. She submitted that OPFS has failed to protect her as their customer.³

In her Complaint with the *Office of the Arbiter for Financial Services*, she explained she was a victim of a scam. In October 2023, she was convinced to invest her money into cryptocurrency with *Hudson Trust*, where she was persuaded to make an initial payment and subsequent payments totalling over GBP £23,000. The Complainant was coached and encouraged by the scammer to create different accounts with various banks as instructed through multiple calls and communications held. The scammer, who had gained her trust, had remote access to her phone through the AnyDesk app and even set up accounts on her behalf (including a 'Roobic' account). She was persuaded this was safe as accounts were in her own name.⁴

She explained her money moved from her account with *Natwest Bank* to *Chase Bank* to *WISE (UK)* and then 'to a new account in [her] name with *Openpayd*'.⁵

The Complainant pointed out that despite the money being transferred to OpenPayd, the latter just stated that she was not their client when she approached it to complain about the payments. The Complainant submitted that she had, however, documentation showing that there was an account in her name with OPFS. She submitted that OPFS failed to protect her.

Remedy requested

The Complainant requested reimbursement of all the money lost. She noted that the last trace of money leaving the WISE a/c to OpenPayd was GBP £23,300.

³ P. 3

⁴ P. 3 & 8

⁵ P. 8 & 9

Having considered, in its entirety, the Service Provider's reply, including attachments,⁶

Where OpenPayd explained and submitted the following:

- That whilst it was unfortunate to hear that the Complainant may have fallen victim to a scam perpetrated by scammers who appear to be operating under the identities of *Andrew Dubinsky* and *Tal Cameron of Hudson Trust*, it referred to its letter to the Complainant dated 25 March 2024 which makes it clear that the Complainant has never been a customer/client of OpenPayd.

The Service Provider submitted that there is no legal or contractual relationship between either (i) the Complainant and OpenPayd nor (ii) Andrew Dubinsky, Tal Cameron (Hudson Trust - www.hudsontrust.co) and OpenPayd, and that the Complainant has misunderstood the services which OpenPayd provides to its corporate customers. It submitted that it is important to note that OpenPayd is not a bank nor a cryptoasset exchange.

It reiterated that the Complainant is therefore not an eligible customer of OpenPayd and, pursuant to the provisions of article 11(1)(a) and article 19(1) of the *Arbiter for Financial Services Act* (CAP. 555 of the Laws of Malta) the Arbiter is to, respectfully, only deal with complaints filed by eligible customers.

Background provided by the Service Provider in its reply

- OpenPayd submitted that it has only ever provided its services to its customers, which include the entities that the letter of the Complainant made reference to, namely:
 - *Octo Liquidity OU* (“SWAPS”); and
 - *GLOBUS SOLUTIONS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ* (“Roobic”).

⁶ P. 83 - 87

It explained that SWAPS and Roobic are cryptocurrency exchanges who, at the time, were customers (the “Merchants”) of OpenPayd.

The Service Provider understands, from the Complainant’s submission, that the Complainant may have entered into commercial agreements with the Merchants and been provided with cryptocurrency wallets with them following communication with the scammer/s.

OpenPayd pointed out that any onboarding would have been conducted solely by the Merchants and OpenPayd would have had no involvement in this and cannot comment on whether or not the Complainant was properly onboarded by the Merchants in question.

OPFS further understands that the substance of the Complainant’s concerns relates to transactions with the Merchant where the Complainant has purchased cryptocurrency. It submitted that any payments to the Merchants by the Complainant for the purchase of cryptocurrency would be a matter between the Merchants and the Complainant as OpenPayd has never provided such services to the Complainant.

OpenPayd’s services

- It explained that OpenPayd is a provider of payment services registered in Malta under company registration number C75580 and is licensed and regulated by the Malta Financial Services Authority (‘MFSA’) as a financial institution in terms of the Financial Institutions Act (Chapter 376, Laws of Malta).
- OpenPayd is not and has never made itself out to be a bank or provider of investment services. OpenPayd provides payment services to its corporate clients (*inter alia* the Merchants) in order to assist them in their own reconciliation of payments.
- It noted that the letter included in the Complaint from WISE suggests that the payments out from the Complainant’s WISE account and paid to the Merchants were paid to ‘bank accounts’ held at OpenPayd. It confirmed that this is not an accurate description of its services – funds were received by OpenPayd as receiving PSP for the Merchants with whom the

Complainant had entered into a contract for the purchase of cryptocurrency.

- It further noted that these clients of OpenPayd may, naturally, have their own onward commercial relationships using these reconciliation services that OpenPayd provides which in this case appears to be between the Merchants and the Complainant.
- OpenPayd submitted that it has never had any commercial or contractual relationship with the unknown scammers who may or may not have operated through the Merchants and/or separately engaged with the Complainant. OpenPayd is not aware, nor could have been or ought to have been aware, of any arrangement between these alleged scammers, the Merchants and the Complainant.
- OpenPayd completed customer due diligence on its customers, SWAPS and Roobic, before they were onboarded and during their relationship as required by applicable laws and regulations. OpenPayd confirms that it complies with all of its anti-money laundering and counterterrorist financing obligations, including undertaking customer due diligence on all its customers. The law states (as has been applied to OpenPayd's business models in a legal opinion prepared for them by Ganado Advocates), that customer due diligence requirements concerning all SWAPS and Roobic's customers are to be performed by SWAPS and Roobic and not by OpenPayd.

Eligibility of complaint

- It further submitted that the Laws of Malta, Chapter 555, provides, in Article 11(1)(a) and again in Article 19(1), that the primary function of the Arbiter is to deal with complaints filed by eligible customers. If the Complainant does not qualify as an eligible customer of OpenPayd, then, the Arbiter is not able to adjudge the Complaint. It quoted that:

"It shall be the primary function of the Arbiter to deal with complaints filed by eligible customers through the means of mediation in accordance with Article 24 and where necessary, by investigation and adjudication".

Whilst Article 2 of the Act defines an ‘eligible customer’ as:

“a customer who is a consumer of a financial services provider, or to whom the financial services provider has offered to provide a financial service, or who has sought the provision of a financial service from a financial services provider.” (emphasis added by OPFS)

The Service Provider noted that the Complainant makes it clear in the Complaint that she was a victim of fraudsters, and OpenPayd is not, in any way, involved in the scam. It quoted the following statements:

“I googled how to find a financial advisor and found Hudson Trust. www.hudsontrust.co the website looks very professional and so I called on 23rd/24th October and spoke to a Finance advisor – Andrew Dubinsky.”

“Andrew then put me in touch with one of his team, I was given a code so I couldn’t speak to the wrong person - Tal Cameron.”⁷

OpenPayd submitted that it does not provide an account, payment or investment service to the Complainant. As such, the Complainant is not “a customer who is a consumer” of OpenPayd.

OpenPayd also confirmed that it has never “offered to provide a financial service” (including, for the avoidance of doubt, any account, payment or investment service) to the Complainant (nor, as OpenPayd only provides its services to corporate clients, could OpenPayd ever have provided any such services to the Complainant) nor has the Complainant “sought the provision of a financial service from OpenPayd”.

It also made it exceptionally clear that the basis on which a number of the Complainant’s concerns seem to be based (that OpenPayd is a bank that has accepted deposits, provided her with a bank account, or that OpenPayd has ‘executed transactions without proper authority’) is similarly entirely incorrect.

⁷ P. 86

OpenPayd reiterated that as there is no contractual relationship between OpenPayd and the Complainant, the Complainant cannot be regarded as an eligible complainant in terms of Article 2 of the Act. It respectfully opined that the Arbiter does not have jurisdiction to deal with the Complaint.

Reply to complaint

- OpenPayd further noted that it promptly investigated the Complainant's initial complaint and, following its investigation, provided the Complainant with its response dated 25 March 2024.
- It submitted that it has, at all times, followed the applicable law and guidance on its obligations in respect of the Complainant's complaint.
- As set out in its response dated 25 March 2024, it remains its clear position that the Complainant should address her concerns to the provider of the service in its regard.
- On the Complainant's specific points raised in her Complaint to the Arbiter, it wished to make it clear that:
 - OpenPayd has no legal relationship with the Complainant.
 - OpenPayd has no relationship whatsoever with the unknown scammers and OpenPayd has had no involvement in any of the interactions that the Complainant has chosen to have with these individuals.
 - In respect of the request to return funds which the Complainant authorised to be paid from her third-party bank account, the Complainant should address this request to the Merchants as beneficiaries.

Preliminary

Competence of the Arbiter

In their reply of 23 August 2024, OPFS raised the plea of the Arbiter's competence to hear the merits of this case.

The Arbiter, after gathering both views on the preliminary plea that challenged his competence, issued a decree on 18 October 2024⁸ whereby he dismissed the preliminary plea and ruled that the Complainant was deemed an eligible customer as defined in Article 2 of CAP 555. As a result, the proceedings continued to hear the Complaint on its merits.

The following table provides an extract from the decree of 18 October 2024:

Extract from the decree of 18 October 2024

...

The hearing

At the hearing of 14 October 2024, the Arbiter invited the Service Provider to explain the rationale of their preliminary plea given the fact that in terms of WISE letter⁹ attached to the Complaint, all the 3 payments complained of were showing the Complainant as the beneficiary not just as the transferor.

Ms Lara Barbuto, on behalf of the Service Provider, explained:

“The Arbiter states that when the service provider received the three transfers, in the letter from Wise (which is a licensed bank in the UK), they give a table on page 1 of the first payment of 16 November (£1,000), 30 November (£18,800) and 12 December (£3,500). They list their beneficiary which is not the company that the service provider mentioned. They say that the beneficiary is [the Complainant].

Yes, because it is the way the model operates from OpenPayd’s perspective. OpenPayd is a provider of virtual IBANs. We are not a bank, so we do not provide bank accounts. We are a payment service provider which acts as a link between our corporate customers and our banking providers themselves. So, we are not in any way a bank ourselves. So, this is not a bank account.

Now, the way this model operates is Octo Liquidity is given a payment account and under that payment account, they can issue virtual IBANs

⁸ P. 97 - 103

⁹ P. 14 - 17

which are linked virtual IBANs in their customers' own names basically. [The Complainant], when she came to make a transfer automatically Octo Liquidity would have issued a linked virtual IBAN in the name of [the Complainant].

However, this is not a bank account. There are no funds in this account. The funds go in immediately and are held within Octo Liquidity's main account. So, it is not a payment account in any way.¹⁰

In her reply, the daughter of the Complainant, who is representing her, stated that in this process, her mum being a vulnerable old age person, was under total control of the fraudster but that her mum knew that the funds were being transferred to OpenPayd and to SWAPS because she found handwritten notes in her mum's record as, for example, p. 75 attached to her Complaint.

When asked by the Arbiter if the Complainant knew that the money was being sent to SWAPS via OpenPayd, the representative replied:

"I say possibly not in that order, but she knew that there were these names of these companies being mentioned along the way."¹¹

Decision re Preliminary Plea

The Arbiter is obliged to give a decision regarding whether he has competence to hear this case before proceeding to hear evidence on its merits.

Having heard the parties and seen all the documents and submissions made, the Arbiter proceeds to decide on the preliminary plea raised by the Service Provider that Complainant is not an eligible customer in terms of Chapter 555 and, consequently, the Arbiter has no competence to adjudge this Complaint.

The transfers complained of show as beneficiary the Complainant and without any reference to any third-party beneficiaries. Nowhere in the transfer payment is there any reference to the Merchant to whose account the Service Provider is claiming to have credited the funds.

¹⁰ P. 93 - 94

¹¹ P. 96

On the contrary, the beneficiary is indicated clearly as being the remitter herself.

In the circumstances, the Arbiter cannot accept that the Complainant:

“never sought the provision of a financial service from OPFS.”

The Arbiter’s competence

Article 22(2) of Chapter 555 of the Laws of Malta (“the Act”) stipulates that:

“Upon receipt of a complaint, the Arbiter shall determine whether the complaint falls within his competence.”

Moreover, in virtue of Article 19(1) of the Act, the Arbiter can only deal with complaints filed by **eligible customers**:

*“It shall be the primary function of the Arbiter to deal with complaints filed by **eligible customers** through the means of mediation in accordance with Article 24 and where necessary, by investigation and adjudication.”*

The Act stipulates further that:

“Without prejudice to the functions of the Arbiter under this Act, it shall be the function of the Office:

*(a) To deal with complaints filed by **eligible customer**.”¹²*

Thus, the Arbiter has to primarily decide whether the Complainant is in fact an **eligible customer** in terms of the Act.

Eligible customer

Article 2 of the Act defines an “eligible customer” as follows:

*“a customer who is a consumer of a financial services provider, or to whom the financial services provider has offered to provide a financial service, or **who has sought the provision of a financial service from a financial services provider**.”¹³*

¹² Article 11(1)(a)

¹³ Emphasis added by Arbiter

Decision

Considering the above and having reviewed the circumstances of the case in question, the Arbiter cannot accept the Service Provider's pretension that the Complainant never sought a service from them. The fact that the transfers were showing the Complainant as the beneficiary, *prima facie* implies she was seeking a service from the Service Provider.

This is irrespective of whether the Complainant was also a customer of the Merchant, being a customer of OPFS, which will be considered further when proceeding with hearings on the merits of the case.

Accordingly, the Complainant is deemed to be an "*eligible customer*" in terms of Article 2 of the Act.

Therefore, the Arbiter has the necessary competence to deal with the merits of this Complaint.

...

Further support to "eligible customer" status emerging from proceedings on merits

The Arbiter would, furthermore, like to add in this decision that the evidence produced and information emerging during the proceedings of this case gives further credence and support to the position that the Complainant qualifies as an "*eligible customer*" for the purposes of Cap. 555.¹⁴

Whilst there may be no legal obligation to conduct customer due diligence by OpenPayd on the merchant's clients' (as may have been outlined in the legal opinion prepared to OPFS referred to in its reply),¹⁵ such aspect, however, relates purely to obligations relating to anti-money laundering and countering the financing of terrorism.¹⁶

¹⁴ Other explanations about the operation of the virtual IBAN's are outlined and quoted later on in this decision in the section dealing with the merits of the case.

¹⁵ P. 85

¹⁶ Even if such legal opinion specifically covered virtual IBANs (which is not evident as no copy was presented), in any case, the aspect of anti-money laundering checks for virtual IBANs is not such a clear-cut matter either as emerging from the EBA Report on Virtual IBANs – EBA/REP/2024/08 – May 2024 (E.g. Sections 3.3/ 3.4 and para.47 / 48 of the said report).

The point raised that OpenPayd was not required to undertake due diligence on the clients of its merchants for AML purposes should not, however, be taken to mean that in the context of virtual IBANs, such underlying clients are automatically excluded from being an ‘eligible customer’ for the purposes of Cap. 555. The latter is a distinct matter that merits to be considered in its own right.

The Arbiter further points out that it cannot also be ignored or discounted that the Complainant was intrinsically deemed as a customer of OpenPayd even by the payment service provider of the Complainant, WISE UK, as clearly emerging in the final response that WISE sent to the complaint made by the Complainant with WISE. In its reply of 1 March 2024, WISE replied:

‘Our Investigation

*From my investigation, I found that you have fallen victim to an impersonation scam. Having read your report, I understand that a financial advisor helped **open another bank account with Openpayd on your behalf** and the funds you lost to the scam **were sent to this account on your name.** To support the transfers, the funds were transferred from your external bank account to Wise and then to Openpayd which were created by the scammer.*

*Transfers **sent to your Openpayd account***

*Once a transfer is sent out to the recipient bank, the funds are no longer under Wise’s control. **For the purpose of these transfers the recipient is a customer of the recipient bank ...***

*... Once we were made aware of **the recipient bank account created on your name** possibly being used for scam purposes’.¹⁷*

Whilst OpenPayd is not a bank, and such references were incorrect, it is clear, however, that WISE considered the transfers to be made to the Complainant as a customer of another payment service provider, OpenPayd.

It is also noted that the reply issued by WISE indicated the Complainant as being the ‘Beneficiary’ for all of the three disputed transfers. The ‘Purpose chosen’ for the transfer was to ‘Yourself’ for the largest payment of GBP 18,800 of 30

¹⁷ P. 14 & 15 – Emphasis added by the Arbiter

November 2023.¹⁸ The ‘GBP statement’ issued by WISE for the period up to 4 December 2023, also indicated the transfer outs (of GBP 1,000 and GBP 18,800) as ‘Sent money to [name of the Complainant]’.¹⁹

The ‘screenshots of payments received from the Complainant’s WISE account as seen on the portal of [OpenPayd’s] banking partner (Clearbank) through which the transactions were received and processed’, as presented by the Service Provider in its final submissions, additionally indicate the ‘Beneficiary Account’ being in the name of the Complainant, the same as for the ‘Remitting Account’.²⁰

Whilst there was no payment account in the name of the Complainant with OpenPayd (as explained by OpenPayd’s representative during the hearing of 14 October 2024), the payment account was given to *Octo Liquidity* who was given the facility by OpenPayd to issue virtual IBANs within OpenPayd’s payments infrastructure with the resulting consequences. During the said sitting it was *inter alia* explained that:

*‘OpenPayd is a provider of virtual IBANs ... Octo Liquidity is given a payment account and under that payment account, they can issue virtual IBANs which are linked virtual IBANs in their customers’ own names basically ... I say, there will be a named virtual IBAN which is not a payment account in the name of [the Complainant] but it is under the whole account of Octo Liquidity’.*²¹

In the sworn declaration of 18 November 2024, the Director and Compliance Officer of OpenPayd further explained the operation of virtual IBANs as follows:

‘(4) As detailed in our reply to the Complaint, OpenPayd provides services to and only has a contractual relationship with corporates. In this case, OpenPayd provides SWAPS with an e-money account that can be used by SWAPS to receive and make payments from third parties (such as the Complainant) in return for the purchase or sale of crypto-assets.

(5) OpenPayd enable corporate customers like SWAPS to have an e-money account with a virtual IBAN (“vIBAN”) attached to them. The e-money account shall, for the purposes of this declaration, be referred to as Merchant E-Money Account. The use of vIBANs has expanded rapidly in

¹⁸ P. 16

¹⁹ P. 60

²⁰ P. 170

²¹ P. 94

recent years and are often used by corporate entities to automate payment reconciliation or to facilitate the tracking of incoming payments.

(6) In simple terms, an IBAN²² is an international payment account number identifier which identifies an individual payment account. Therefore there is one physical account linked to an IBAN. In contrast to a traditional IBAN, virtual IBANs are not directly linked to a single bank account, but rather any number of virtual IBANs (sub-IBANs) can be issued. The vIBAN system directs incoming payments to one designated 'master' IBAN and corresponding bank account. OpenPayd maintains a physical bank account and associated IBAN through its banking partner. This account is dedicated to safeguarding client funds. The banking partner not only manages the origination of this account but also authorises OpenPayd to allocate vIBANs linked to it.

(7) SWAPS (and [many] other corporate customers of OpenPayd) have one Merchant E-money Account with one unique "master" vIBAN and with multiple "linked" vIBANs which are allocated to SWAPS end customers. One important aspect to consider is that virtual IBANs look identical to IBAN codes but do not have the capacity to hold any actual balance; they are only used to re-route incoming payments to a regular IBAN linked to a physical bank account. All payments made towards a vIBAN are credited directly to the physical bank account – in this case – OpenPayd's safeguarding account ...'.²³

Although the Complainant did not herself have a payment account with OpenPayd, she was ultimately allocated a sub-account or a linked account within OpenPayd's systems and payments infrastructure.

OpenPayd's contestation that no consumer relationship existed rather corroborates (and needs to be seen and considered also in the context of), the risks and challenges of virtual IBANs as highlighted by the European Banking Authority ("EBA"). Various matters raised by the EBA in its 'Report on Virtual IBANs' of May 2024 - EBA/Rep/2024/08 ("the EBA Report") (which shall be

²² Definition of IBAN in the SEPA Regulation (EU) No. 260/2023 which establishes technical and business requirements for credit transfers and direct debits in euro and amending Regulations (EC) no. 924/2009.

²³ P. 111 - 112

considered in detail later in this decision), are indeed relevant to the considerations in question.²⁴

At this stage, it is to be pointed out that the divergent interpretations and lack of clarity involving virtual IBANs (“vIBANS”) and ensuing consumer relationships was *inter alia* itself highlighted in the EBA Report on Virtual IBANs. The EBA even suggested clarifying the definition of a ‘payment account’ in the Payment Services Directive²⁵ (“PSD2”) to clearly capture vIBANs to mitigate such risks. For example, the EBA Report outlined *inter alia* that:

“70. If the vIBAN is deemed as an identifier of the master account to which it is linked, as explained in paragraph 12 above, then where the end users of the vIBANs are not the holder of the master account, the master account cannot be deemed as the payment account of those end users, since it is held in the name of another person. This is because PSD2 defines a payment account as ‘an account held in the name of one or more payment service users which is used for the execution of payment transactions’ (Article 4 (12) of PSD2).

71. In such cases, a risk arises that those end users may not have a payment account, within the meaning of PSD2, and therefore they may not benefit from all the safeguards and rights in PSD2 associated with having a payment account (including in terms of disclosure requirements, application of strong customer authentication and access by account information and payment initiation service providers to payment accounts).

72. Where the end users of the vIBANs do not have a payment account, this also has ramifications about the legal qualification of the payment services provided by the respective PSPs to the end users (e.g. as money remittance vs credit transfers). In this regard, while money remittance implies that no payment account is created in the name of the payer, a credit transfer implies that funds are transferred from the payer’s payment account. This creates a risk of divergent interpretations across NCAs about the qualification of the payment

²⁴ European Banking Authority (EBA) Report on Virtual IBANs – EBA/REP/2024/08 – May 2024
<https://www.eba.europa.eu/sites/default/files/2024-05/612f03de-965a-4157-b638-1b4c5b081f87/EBA%20Report%20on%20virtual%20IBANs.pdf>

²⁵ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.

services provided by the PSPs offering the vIBANs to the end users, in the specific case mentioned above, which can lead to an unlevel playing field and regulatory arbitrage issues.

73. *The risk could be mitigated by the PSD2 clarifying the definition of a ‘payment account’ and in particular whether users of vIBANs that are not the holder of the master account holder, such as in Use Cases 2 and 3 above, are considered to have a payment account within the meaning of PSD2.”*

The points raised further support the basis and justification for the consideration of a consumer relationship *de facto* existing between the Complainant and OpenPayd, as ultimately seen and understood not just by the Complainant herself,²⁶ but even by WISE UK as the Complainant’s payment service provider.

In the circumstances, the Arbiter considers that the required criteria applicable to an ‘eligible customer’ for the purposes of Cap. 555 as defined in Article 2 of the Act are, in substance and essence, deemed to be satisfied in the Complainant’s case in the context of virtual IBANs and the manner how this operated in practice.

The argument that the Complainant is not an ‘eligible customer’ just because she did not have a payment account herself but only allocated a virtual IBAN is not deemed justified in the circumstances considering that the payment orders identified her as the beneficiary and also the debates on the risks and challenges of this area and also the spirit of the law.

The provision of virtual IBANs is ultimately a relatively novel and particular financial service offered by OpenPayd for which it is ultimately responsible.

The Arbiter would like to add that he has seen and decided other cases in favour of the Service Provider, which may initially look similar but are quite distinct from the case in question.²⁷

²⁶ The Complainant’s impression that she was the beneficiary of the account with OpenPayd further emerges in the call log produced by the Complainant as attached to her email to the OAFS of 20 December 2024 (P. 137, 143, 144 & 146 refer).

²⁷ Example:

ASF 70/2024 - <https://financialarbiter.org.mt/sites/default/files/oafs/decisions/1842/ASF%20070-2024%20-%20ZJ%20vs%20OpenPayd%20Financial%20Services%20Malta%20Limited.pdf>

ASF 112/2024 - <https://financialarbiter.org.mt/sites/default/files/oafs/decisions/2037/ASF%20112-2024%20-%20CA%20vs%20Openpayd%20Financial%20Services%20Malta%20Limited.pdf>

ASF 135/2024 - <https://financialarbiter.org.mt/sites/default/files/oafs/decisions/2122/ASF%20135-2024%20-%20HC%20vs%20Openpayd%20Financial%20Services%20Malta%20Limited.pdf>

All other cases (where the Arbiter accepted the Service Provider's plea about his competence, given the complainant was not deemed an eligible customer for the purposes of the Act) involved material differences to the case under consideration as pointed out. In those other cases, either the issue of the virtual IBANs did not transpire (in the way it has emerged in the Complainant's case); and/or the third-party corporate client of OPFS had been clearly and solely named as the beneficiary in the payment order (contrary to the Complainant's case where she was the only beneficiary featured in the payment order) and also in such other cases there was clear evidence that the remitter had clear and ample knowledge that the funds were being transferred to the corporate client of OPFS and not to a payment account in their name. In such other cases, the complainant was furthermore never as vulnerable as the Complainant.

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.²⁸

The Arbiter is considering all pleas raised by OpenPayd 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 555²⁹ which stipulates that he should deal with complaints in '*an economical and expeditious manner*'.

Asserted scam

The Arbiter 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, there is sufficient comfort that the Complainant had fallen victim to a scam.

Consideration has, in this regard, been given to various factors including: the particular circumstances of this case; the nature and credibility of the events as outlined in the Complaint and the testimony and the evidence produced; the call logs with the scammer;³⁰ the activities of *Octo Liquidity OU* (trading under

ASF 206/2024 (not yet uploaded on OAFS's website)

²⁸ Cap. 555, Art. 19(3)(b)

²⁹ Art. 19(3)(d)

³⁰ P. 21 - 28 & 42 - 49

the name SWAPS in Estonia), which involved cryptocurrency (and with Octo seemingly no longer remaining a customer of OpenPayd);³¹ the apparent lack of regulatory status of *Octo Liquidity OU* ('Octo') which did not feature as a supervised entity on the website of *Finantsinspektsioon* (the financial services regulator in Estonia)³² despite the statement on Octo's website that "*Swaps is a fully regulated business. We are registered in Estonia*";³³ copies of exchanges with SWAPS;³⁴ and official payment statements produced.³⁵

Other hearings

At the hearing of 4 November 2024, *EE* confirmed that her mother (Complainant) has:

"... MS and this has significantly affected her mental health because she has lost all her money in this scam and is facing having to move out of her home. So, every time that all of this is discussed, she spirals into a severe depression."³⁶

EE also stated she has no further proof to present other than what is filed in the Complaint and what she had stated in the first hearing of 14 October 2024, namely:

"I think by the time this had all happened, my mum was completely above any form of making any decisions or knowing what was happening because she was being controlled by this person who was the scammer, and she was telling her to make these transactions. She was showing mum what to do. She was giving her scripted messages of what to say when she was ringing up banks, persuading them to allow her to make these transactions, overriding scam warnings. She told her, 'This happens all the time. Trust me. I'm here to help you. We're going to make money'. And she was constantly spinning this yarn in her ear."

³¹ P. 84

³² <https://www.fi.ee/en/supervised-entities?closed=1&keys=Octo%20Liquidity>

³³ <https://help.swaps.app/en/articles/5206942-is-swaps-a-regulated-business>

³⁴ E.g. P. 52 - 53; 55 - 56 amongst others

³⁵ P. 60 - 74

³⁶ P. 104

The Arbiter states that in my narrative, it seems that she knew to whom she was transferring the money, to somebody trading under the name of SWAPS.

I say only in the sense that she'd initially sought some help for investing in what she felt was an appropriate thing to do to invest in cryptocurrency. So, the whole start of this process was that she had seen a local presenter who is supposed to be a money expert suggesting that people invest in cryptocurrency. That in itself had been a scam that she had seen.

The Arbiter is referring to part of (the Complainant's) complaint (p. 9) which says:

"She told me that she was going home for Christmas to Poland to meet her Mum and Dad and 3 sisters and said it would be advisable to put the money into the hands of "SWAPS".

So, when making these transfers, she was aware that this money was intended to be sent to SWAPS.

I say, she did but she did not understand what SWAPS meant.

She was totally under the control of the fraudster.

She did know about SWAPS before transferring the money.

Asked whether she knew about OpenPayd at that time, I say she's written some notes down about OpenPayd because she's written account numbers saying that she's a beneficiary, but to a layman a person being called a beneficiary versus an account holder, she doesn't understand the difference between those. She just was writing down what she thought was her account number. So, she has written about OpenPayd in her notes at the time when she was speaking to the scammer.

It is said so she knew that the money was being sent to SWAPS via OpenPayd.

I say possibly not in that order, but she knew that there were these names of these companies being mentioned along the way."³⁷

³⁷ P. 95 - 96

Upon cross-examination during the second hearing of 4 November 2024, EE continued:

“It is being said that in the complaint, I started by saying that my mother was a victim of a scam.

Asked whether it is correct to say that my mother found Hudson Trust herself online and that she had contacted them herself showing an interest in cryptocurrency, I say that that is correct to the point that she had fallen for a scam of a local money saving expert in the UK called Martin Lewis who ‘supposedly’ advised people to invest in cryptocurrency. And that, in itself, had been a scam.

But the way that my mother’s health was at the time, led her to panic about the money that she had left in her bank, and she wanted to try and do something about it. She had always gone to her brother for financial advice before and the brother she used to go to passed away a few years ago. So, she did not have that person anymore. She lives on her own and she has always been fiercely independent and has very rarely wanted to ask me for advice because she’d seen that as a weakness.

And, so, she did all of this because she wanted to try and make some more money from the money that she had left. And as there were a lot of people around her dying, and she did not want to end up with no money; and she was foolish in not researching and not taking advice.

It is being said that in the emails it seems that my mother first put in £200 in her account thinking that within two/three weeks she was supposedly going to make £349.

Asked why when that money was not received initially, she continued investing in this crypto without any returns and continued sending money to the same account, I say that she wouldn’t know how to check. She’s very, very poor with technology. She has never used a banking app and she often misses going to the bank branch because of her MS, and she does not get up very early in the morning. So, by the time she goes out to the bank, it is closing time.

She just believed what she was being told and she did ask but was not sent any information. She was being fobbed up all the time saying that she will get her return and she would get the money and my mum trusted

this person. She's got a very trusting nature, and this person has essentially groomed mum into building up that trust.

It is being said that in the emails there were a number of authentication passwords and verification documents which were asked for. Asked whether my mother would share all these codes with the financial advisor; if the merchant would send a code to verify whether she would share all this with the alleged financial advisor, I say that no, she wouldn't know how to.

So, they made her download Anydesk app which allows the scammers access to mum's phone, as all this was done in the background, without mum knowing what was going on. Mum does not know the difference between Whatsapp and a text message. There is no way that she would be able to send and do that. So, there are emails that I found going through mum's phone, so I sent them in terms of timelines and all the things that have been going on in the background because it has been such a complex web of transactions.

It is being said that when we complained to WISE, they said that they sent a transaction report (on page 16 of the complaint) where they confirmed that the payment instructions came from the details that they had pertaining to my mother, and they said that there was a scam warning which she ignored.

Asked whether I know anything about this, I say she raised this quite a few times with the scammer and she was always reassured that this was a common thing that happens. You just need to override it.

Asked whether she told the scammers about this warning, I say, yes. It is written in the call log, and you can see that she said, 'They are warning me,' and the scammers had reassured her that 'It happens all the time. We can sort this. We can do this. We are so close now. Your investments are growing. We just need to get on and do this.' Those sorts of things."³⁸

...

"It is being said that on the transaction that my mother made she indicated that the funds were going to herself.

³⁸ P. 105 - 106

I say that she didn't make those transactions; she wouldn't know. All she's done is being the person who has been in the background, so she did not choose to make them. She did not even set up the bank details or the account details with OpenPayd as a beneficiary. She was given them, and this is proven in the call log. The scammer has given mom those details of her account – name and details.

So, mum did not set them up; the scammers had done it.

It is being said that OpenPayd is not a bank and does not hold the money and that the IBAN number was the merchants', of Octo Liquidity and Roobic.

I say that this does not make any difference to a layman person who thinks that they are investing in something. Even I wouldn't know or understood this.

What you've got to try to understand is that, ultimately, you've got a vulnerable person who is just trusting what is being told to her. And if it has been explained by the scammer that it's going to this bank next and to this bank, that was how it was explained.

I say my mum has not chosen OpenPayd, she has not chosen Swaps. She has not chosen anything; the only thing she chose was Hudson Trust and that was due to her naivety.

It is being said that the bank numbers (the bank IBAN or code) were given to her by the person who was communicating with her, by the financial advisor.

I say, yes."³⁹

Following this hearing, the Service Provider presented a Sworn Declaration⁴⁰ explaining why and how the funds remitted by Complainant were credited to the account of their corporate clients *Octoliquidity OU* (trading as SWAPS) and *Globus Solutions OO* (trading as ROOBIC) even though the beneficiary of the payment orders received from WISE reportedly showed as beneficiary the

³⁹ P. 107

⁴⁰ P. 111 - 126

Complainant herself, without any mention of the concerned corporate clients of OPFS.

This in accordance with the system referred to as virtual-IBANs, which is not covered by specific regulation.⁴¹

At the hearing of 3 December 2024, the Service Provider represented by Andre Schembri submitted:

“I say basically what happens is this. SWAPS was our client and any kind of merchant can be our client. We set up an account for them and, depending where they want to operate, we can give them links, IBAN or else an account wallet.

But let us stick to this one. If an individual wants to make use of the services of SWAPS, the first thing they would do will start a customer relationship with them. And that would involve the client going to the individual customer and going to the websites. And through there, they open an account with SWAPS and that would entail the customer providing certain details which may vary from merchant to merchant but, let’s say, it would be name, surname, address, ID, some form of verification to SWAPS.

Then, from their end, SWAPS can, since they were a customer of OpenPayd, relay certain information to the OpenPayd system in order to create what we call a linked vIBAN. The linked vIBAN is associated with the details provided by SWAPS. So, if SWAPS say, ‘Listen, please create a vIBAN with the name of XYZ,’ the OpenPayd system can create that vIBAN.

The purpose of the linked vIBAN is to facilitate the payment for the end customer to SWAPS via bank transfer. So, then, if the customer wants to proceed and invest some of his/her money with SWAPS, what would happen is that the customer would go to their banking portal, whichever bank that may be, HSBC, Barclays, whatever (in this case it was WISE),

⁴¹ In May 2024, the European Banking Authority has issued a Report reference EBA/Rep/2024/08 REPORT ON VIRTUAL IBANs where it *inter alia* highlighted certain risks applicable to virtual IBANs such as ‘risks that consumers may be misled to think they are paying to an account held in one country (e.g. their own country), which may give more comfort to the consumer, when in fact the funds are transferred to a master account in a different country’ (page 26 of the Report).

and there instruct a transfer from their account to the linked vIBAN that SWAPS provides to the individual customer.

The customer would input the details and their banking portal, whichever bank they operate with, and they would instruct the transfer. Once the transfer gets executed from their bank, goes through the payment scheme and hits the OpenPayd system, the OpenPayd system knows that the link with the virtual IBAN is linked to SWAPS and automatically that money is transferred as rerouted to the main account of SWAPS.

So, that is the way the money flows.

If the client, the customer, wants to invest, let's say, in cryptocurrency, then it is up to SWAPS to make the movement to the cryptocurrency exchange and buy the cryptocurrency.⁴²

Following this explanation and other subsequent explanations during the said hearing of 3 December 2024, the Arbiter remarked:

"The Arbiter states that the client⁴³ is not part of this complaint. This complaint is between [the Complainant] and OpenPayd. So, [the Complainant] is asking: 'I sent money to myself with you,' and instead of saying, '(Complainant), you do not have an account with me. I'm going to send this money back,' OpenPayd just took the liberty to put the account, the funds, in the name of a third party who's not mentioned in any way in the transfer.

That is what the Arbiter understands.⁴⁴

The Arbiter insisted on having information from the Service Provider whether in the payment orders received from WISE there was any reference to their corporate clients to whom they credited the transfers, which had shown the Complainant as the beneficiary.

The Arbiter further stated:

"I need to understand what instructions were sent by WISE to OpenPayd. I have the letter of WISE and that is the only letter that I have.

⁴² P. 128

⁴³ In this context client refers to the corporate client of OPFS.

⁴⁴ P. 130

OpenPayd have shown in their submissions a lot of documentation which is generated internally which obviously pick up the vIBAN number and generates that. But I want to understand exactly what information was received from WISE.

The Arbiter requests [EE] to send the Call Log again in its entirety to the secretary for distribution to the parties concerned.

The Arbiter requests Mr Andre Schembri to confirm exactly what they received from WISE (not how it was processed internally).

WISE, in their communication for the payment, apart from giving the IBAN number, they made reference to a name. The Arbiter wants to know who the beneficiary is because, ultimately, he is relying on a WISE letter, but he wants to see exactly what they sent to ensure it corresponds to what they are saying.

The Arbiter states that the whole issue is who was the beneficiary of that transfer and whether OpenPayd were correct in ignoring that beneficiary and putting it into a third-party name with whom the beneficiary might have had an account.

The Arbiter wants to know what instructions OpenPayd received from WISE.

The Arbiter requests from the complainant the document – Call Log – she referred to earlier.

The Arbiter requests from the service provider evidence of the instructions received from WISE showing who was the beneficiary of this transfer.”⁴⁵

Final submissions

Preceding her final submissions,⁴⁶ EE submitted (as requested by the Arbiter) eighteen pages of call logs between her mother and the fraudsters⁴⁷ making particular reference to instructions from fraudsters mentioning OPFS, namely:

⁴⁵ P. 135

⁴⁶ P. 158 - 159

⁴⁷ P. 137 - 155

“09/11/2023 at 12:51:11

Beneficiary Name: [the Complainant]

Account number: xxxxx895

Sort code: xxx679

Bank name: Openpayd Financial Services LTD

Bank Address: 133 Houndsditch, London EC3A 7BX, United Kingdom

Reference ID: 44a07a68.”⁴⁸

Same information was repeated on **09/11/2023 at 17:04:03⁴⁹** and on **15/11/2023 at 13:21:38.⁵⁰**

Consequently, the Complainant argued that the Service Provider had no right to credit the funds transferred to an account in the name of the Complainant with a third party who is not named in the transfer order. She stated:

“Misleading Transfer Details: The transaction details and account information presented to (the Complainant) during the transfer process appeared legitimate. It looked like the money was going to OpenPayd account and would be credited to her own account. SWAPS is not mentioned at all. As no Openpayd account existed, the funds should have been returned.”⁵¹

In their final submissions,⁵² OPFS, while re-explaining their business model and how vIBANS operate, claimed that they have no obligation to match the beneficiary named in the transfer to the vIBAN account holder quoting article 88 of PSD2 Directive (reproduced in Central Bank of Malta (CBM) Directive 1 Section 3 Liability – 63 [1]) which states:

⁴⁸ P. 143 - 144

⁴⁹ P. 144

⁵⁰ P. 146

⁵¹ P. 159 – Emphasis added by the Arbiter

⁵² P. 162 - 170

“if a payment order is executed in accordance with the unique identifier, the payment order shall be deemed to have been executed correctly with regard to the payee specified by the unique identifier.”⁵³

The Arbiter has given specific authority for the argument regarding regulatory authority to credit funds to a beneficiary account not named in transfer to be treated in the final submissions.⁵⁴ Therefore, the Arbiter will consider these arguments, which were made in the final submissions, in his next analysis which will lead to the decision.

Analysis and consideration

In terms of Article 19(3)(b) of CAP. 555 of the Laws of Malta, the Arbiter shall determine and adjudge a complaint by reference to what, in his opinion, is fair, equitable and reasonable in the particular circumstances and substantive merits of the case.

In the proceedings, it has emerged clearly that the Complainant was unquestionably a vulnerable, old person who was being aggressively manipulated by fraudsters. The latter carefully cultivated her trust to the point of extracting her authority for total control of her communications with banks whereby her funds were transferred between UK banks⁵⁵ until they were transferred by Chase to an account in the Complainant’s name with WISE in UK through four transfers dated 15, 21, 29 November 2023 and 12 December 2023.⁵⁶

For the purpose of this Complaint, what really matters is the process whereby funds were transferred from Complainant’s account with WISE and how with the intervention of OPFS these ultimately finished in the accounts of ROOBIC and SWAPS held with OPFS. From there, the funds came under full control of the fraudsters who, having clinched their reward, evaporated into thin air.

Payments between banking and payments institutions in UK are governed by an elaborate complaint handling procedure issued by the UK regulator Financial

⁵³ P. 165

⁵⁴ P. 132; 133; 135; 156

⁵⁵ From Natwest to Chase and then to Wise - p. 60 - 74

⁵⁶ P. 69 – 71; p. 60

Conduct Authority (FCA)⁵⁷ commonly referred to as DISP (Dispute Resolution). This explains how complaints unless resolved in accordance with the set procedures can be referred for resolution through the UK Financial Ombudsman (FSO).

In cases of fraud scams complaints, FSO generally protects consumers where a UK financial institution allows payments by an inexperienced investor directly to a crypto exchange. The following extract from the FSO's website, for example, refers:

'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.

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.⁵⁸

In the case of this particular Complaint, however, the payment was made from NATWEST to CHASE, from CHASE to WISE and then, from WISE to OPFS (using their UK address and thus offering a service in the UK).

In all these strings of payment, the beneficiary was shown to be the remitter herself with no indication that there was going to be either a change of beneficial ownership of the funds being transferred or that the funds would end up from a presumed same beneficiary account with OPFS to an account of an institution not covered by DISP which was essentially a crypto service institution like SWAPS or ROOBIC. Indeed, nowhere did it feature in the payment system that the

⁵⁷ <https://www.handbook.fca.org.uk/handbook/DISP/INTRO/?view=chapter>

⁵⁸ <https://www.financial-ombudsman.org.uk/decisions-case-studies/case-studies/consumer-contacts-us-complain-cryptocurrency-investment-scam>

Complainant's funds were going to be transferred to a third-party account (which third parties were in practice 'cryptocurrency exchanges').⁵⁹

The screenshots of payments received from the Complainant's WISE account as presented by the Service Provider indeed indicated the Complainant's name for the Beneficiary Account.⁶⁰

There is a fair consideration that if WISE had known that the funds transferred to OPFS to credit the account of their client, the remitter (Complainant), were actually being directed to another party, (involving crypto-related transactions), rather than to her own account, then, they would have likely further warned their client and possibly even stopped from executing such transfers.

Any failure by WISE to warn their client or restrict/block the transfers would have quite probably led to a successful case being brought to the UK – FSO who, as the above-quoted example, would have in all probability found in favour of the consumer and ordered full refund.

The fact is that through their internal systems, OPFS took it upon themselves, and just proceeded to credit the funds to the remitter's account with a third-party client of OPFS, which at that point in time was unbeknown to the remitter and also the Complainant's payment provider (WISE UK).⁶¹

The crediting of the funds to the remitter's account of a third-party client of OPFS occurred without seemingly any specific authority from the remitter and/or without proper system warnings/adequate intervention to ensure clarity and transparency about the payment transfers involving a virtual IBAN (and not a transfer to the Complainant's own payment account).

This scenario ultimately resulted in material adverse consequences and lack of protection to the Complainant – *inter alia* resulting in a lack of transparency that the Complainant had no payment account with OpenPayd, and the circumvention or dilution of effective protection and redress that the

⁵⁹ In its reply of 23 August 2024, OpenPayd described 'SWAPS' and 'Roobic' as 'cryptocurrency exchanges' – P. 84

⁶⁰ P. 170

⁶¹ P. 51 - 59 show that direct communication from SWAPS was received by Complainant only after the bulk of the funds remitted (GBP 18,800 out of GBP 23,300) had been directed to their account with OPFS.

Complainant would have had under the UK financial system, prejudicing her position in the process.

The Arbiter considers that innovation should not be used or result in the material detriment of a financial services consumer, even more, a vulnerable consumer as was the Complainant.

Consequently, the Arbiter considers that whilst the innovative systems of virtual IBANs, though unregulated or not specifically addressed in the regulatory framework, have certain benefits which are well explained in the EBA report earlier referred to in this decision, this should not involve or end up denying consumers from payment protection in their home country systems and neither in enabling a system which lacks transparency and/or lack of clarity in the payment process, including in the exchanges between payment service providers.

One needs to, furthermore, stress that the Service Provider had clear regulatory obligations to onboard corporate clients after thorough due diligence of both their own status as well of the robustness of their systems not to allow their abuse by fraudsters apart from obligations to ensure that the virtual IBANs are not operated in a way to the disadvantage and detriment of the end users.

It is noted that, in its final submissions, the Service Provider referred to Articles 88(1) and 88(5) as well as Articles 45(1) and 52(2)(b) of the PSD2 in its defence.⁶² The Service Provider highlighted *inter alia* that:

⁶² - Article 45(1) of PSD 2 provides that: “Member States shall ensure that the following information and conditions are provided or made available by the payment service provider to the payment service user: (a) a specification of the information or unique identifier to be provided by the payment service user in order for a payment order to be properly initiated or executed; ...”

- Article 52(2)(b) of PSD 2 provides that: “Member States shall ensure that the following information and conditions are provided to the payment service user: ... 2. on use of the payment service: (b) a specification of the information or unique identifier that has to be provided by the payment service user in order for a payment order to be properly initiated or executed; ...”

- Article 88(5) of PSD 2 provides that: “If the payment service user provides information in addition to that specified in point (a) of Article 45(1) or point (2)(b) of Article 52, the payment service provider shall be liable only for the execution of payment transactions in accordance with the unique identifier provided by the payment service user”.

*“Once again focus is placed on the fact that payment service providers may rely on the IBAN, or vIBAN linked to a master IBAN, as the unique identifier and that there is no obligation to match or to check for any discrepancy by and between the beneficiary’s name and the IBAN”.*⁶³

The term ‘unique identifier’ is defined under Article 4(33) of the PSD2 as:

“means a combination of letters, numbers or symbols specified to the payment service user by the payment service provider and to be provided by the payment service user to identify unambiguously another payment service user and/or the payment account of that other payment service user for a payment transaction.”

The Arbiter has considered the defence raised by OPFS that they had no “regulatory obligation to verify whether the IBAN and the name of the payee as provided by the Complainant match”.⁶⁴

The Arbiter has to decide whether what applies to normal IBANs in terms of Article 88 of PSD2⁶⁵ and CBM Directive 1 also automatically applies to virtual IBANs which are not specifically covered by the said PSD2 and CBM Directive 1.⁶⁶

The Arbiter relies in his analysis on the EBA Report referred to earlier in this decision.

The very existence of such a Report clearly shows that vIBANS are not covered by what the legislator had in mind when issuing the PSD2. Yet, the Service Provider is using the existing IBAN framework to justify its actions/inactions regarding virtual IBANs.

As stated in section 3 of such Report, vIBANS represented risks and challenges that are specific and additional to normal IBANs. The Report highlights various

⁶³ P. 166

⁶⁴ *Ibid.*

⁶⁵ Directive (EU) 2015/2366 on payment services.

⁶⁶ Article 88(1) of PSD 2 provides that: “If a payment order is executed in accordance with the unique identifier, the payment order shall be deemed to have been executed correctly with regard to the payee specified by the unique identifier.”

risks and challenges arising for consumers ‘stemming from lack of transparency’,⁶⁷ amongst others, as outlined in the said section 3 of the Report.⁶⁸

In particular, the Report refers to *inter alia*:

*“risks arising for the end users of vIBANs where they are not the master account holders, and associated unlevel playing field and regulatory arbitrage issues stemming from divergent interpretation across NCAs about the qualification of the relevant payment services in such cases;”*⁶⁹

*“risks of vIBANs being used by non-EU financial institutions or by EU non-PSPs to provide payment services without the required authorisation;”*⁷⁰

*“risks arising for consumers using vIBANs and for consumers making a payment to a vIBAN, stemming from lack of transparency;”*⁷¹

*“risks arising to users of vIBANs stemming from inappropriate disclosure about which DGS [Deposit Guarantee Scheme] protects their deposits, and risks arising to DGSs.”*⁷²

It is noted that the EBA Report of May 2024 explains that,

*“There is currently no legal definition of vIBANs at EU level, and no uniform understanding across NCAs and the industry of what vIBANs are.”*⁷³

The said EBA Report also stated *inter alia* that:

*“For third parties, vIBANs are typically indistinguishable from a regular IBAN. For example, where a payment is made by a payer to the user of a vIBAN, the payer’s PSP would not be able to discern that the account identifier provided is a vIBAN (instead of a regular IBAN), and will not know the master account to which the funds are transferred.”*⁷⁴

⁶⁷ P. 26 of the EBA/Rep/2024/08

⁶⁸ P. 12 to 28 of the EBA/Rep/2024/08

⁶⁹ P. 12 of the EBA/Rep/2024/08

⁷⁰ P. 13 of the EBA/Rep/2024/08

⁷¹ *Ibid.*

⁷² *Ibid.*

⁷³ Point 6, Page 6 of the EBA Report on vIBANs

⁷⁴ Point 13, Page 7 of the EBA Report on vIBANs

The Arbiter also notes the explanation provided under section 3.6 of the EBA Report which deals with the risks for end users of vIBANs where they are not the master account holder as outlined earlier in the preliminary plea section.

The Arbiter also notes the matters raised by the EBA in section 3.11 of the Report related to risks for consumers making a payment to a vIBAN, stemming from lack of transparency, in particular:

95. In addition, vIBANs can also increase risks for consumers in case of inappropriate disclosure in the pre-contractual information, which may lead to consumers not understanding the product/service they are contracting, or in case of inappropriate disclosure in the contractual information for vIBANs.

97. vIBANs may also raise risks and challenges for consumers making a payment to a payee which uses vIBAN. These include:

- risks that consumers may be misled to think they are paying to an account held in one country (e.g. their own country), which may give more comfort to the consumer, when in fact the funds are transferred to a master account in a different country.*
- challenges in the enforcement of consumer claims towards the payee, and in the prosecution of fraudulent activities, especially where the vIBAN and the IBAN of the master account have different country codes.⁷⁵*

It has not emerged in this case that throughout the service of vIBANs, the Service Provider has reasonably ensured that there was transparency in the payment process and offer of the vIBAN financial service.

The Complainant as the end user of the vIBAN and her payment service provider were not aware that the Complainant had no payment account in her name with OPFS but that the transfer involved a virtual IBAN with the ensuing implications.

⁷⁵ P. 26 – 27 of the EBA/Rep/2024/08

As explained earlier on, it clearly emerged that there was a lack of clarity, information and transparency in the use and application of the virtual IBAN.⁷⁶

Consequently, the Arbiter does not accept the Service Provider's defence that their action to credit the funds in question to a beneficiary not named in the transfer order was adequately covered and satisfied the provisions of the PSD2 and CBM Directive 1 referred to earlier and/or reflected the general principle of transparency advocated in the PSD2 and/or ultimately reflected the legitimate and reasonable expectations of consumers.

In light of the lacunae and lack of uniform understanding, approach and transparency about virtual IBANs as clearly emerging from the EBA Report, it was even more necessary, as well as only reasonable and legitimate to expect OpenPayd to have taken appropriate action and adequately intervened in the payment process or ensured in some other way that there was clarity to the user of the vIBAN (and her payment service provider) who had indicated herself as the beneficiary in the payment order about the nature of the service and transactions.

This was in the interest and for the protection of payment service user, fraud prevention and integrity of the payment system.

The information involving the transfer of funds was ultimately misleading or incomplete and did not ensure a clear and adequate understanding by the Complainant and her payment service provider.

The Arbiter does not accept that the Service Provider has no responsibility for the damages suffered by the Complainant when it was the Service Provider who offered and enabled the vIBANs service to the third party and, also, given the way the vIBAN was applied to the Complainant's detriment as amply explained above.

This is particularly so when the named beneficiary in the transfer orders was the Payer herself as also amply described and evidenced in this decision.

⁷⁶ Even if, for argument's sake, vIBANs were covered by the same regulation provisions of IBANs, it is doubtful if the protection would apply in cases where the remitter names himself as the beneficiary while the IBAN belongs to a third party in the same way that it applies where the beneficiary is a third party who is different from the holder of the IBAN account.

By its very nature, this *inter alia* resulted in a reduced level of transaction monitoring protection, as provided under the PSD2 and regulations applicable in the UK financial system, on the part of the remitter's bank/payment institutions on the presumption that the transaction represented a 'me to me' payment to a licensed EU institution without any change of ultimate beneficiary when this was not the case in reality.

In this particular case, a 'me to me payment' had already happened twice when funds were transferred from Natwest to Chase and then from Chase to WISE, and there was a fair presumption on the part of WISE that the same would happen when they transferred funds to OpenPayd seemingly believing that the transfer involved another payment to the Complainant's own account when this was not truly the case.

Decision

For the reasons stated, the Arbiter considers the Complaint to be fair, equitable, and reasonable in the particular circumstances and substantive merits of the case and is accepting it in so far as it is compatible with this decision.

In accordance with Article 26(3)(c)(iv) of Chapter 555 of the Laws of Malta, the Arbiter accordingly orders *OpenPayd Financial Services Malta Limited* to pay to the Complainant the sum of GBP 23,300 (twenty-three thousand, three hundred pounds Sterling).

With interest at the rate of 4.5% p.a.⁷⁷ from the date of this decision till the date of payment.⁷⁸

The costs of these proceedings are to be borne by the Service Provider.

Alfred Mifsud
Arbiter for Financial Services

⁷⁷ Equivalent to the current Bank of England Bank Rate.

⁷⁸ 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.

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.

Costs of the proceedings

In terms of article 26(3)(d) of Cap. 555 of the Laws of Malta ('the Act'), the Arbiter has adjudicated by whom the costs of the proceedings are borne and in what proportion, taking into consideration the particular circumstances of the case.

The costs of the proceedings are not limited to the payment of any applicable cost of filing the Complaint with the Office of the Arbiter for Financial Services (previously Eur25) but may also include any reasonable lawful professional and legal fees paid by the Complainant limited to the acts filed during the proceedings of the case. Such professional fees should not include any contingency judicial fees and charges.

The extent of tariffs and fees in respect of professional or consultancy services rendered to customers in relation to the claims or proceedings under the Act, that may be lawfully and reasonably requested as part of the said costs of proceedings, are not defined in the current provisions of the Act.

However, the Arbiter expects these to be benchmarked on tariffs and fees as stipulated and applicable for Civil Court proceedings in Malta under the Code of Organisation and Civil Procedure.