Before the Arbiter for Financial Services

Case ASF 054/2025

ZO

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris' or 'Service Provider')

Sitting of 20 February 2026

The Arbiter,

Having seen the Complaint made against Foris DAX MT Limited relating to its alleged failure to warn client that his transfer of digital assets (which digital assets were funded by transfer of Euro currency from his bank accounts with Caisse d'Epargne and Banque Populaire (France) from his account with Service Provider) to a fraudulent platform, has caused him a financial loss for which he is seeking compensation of €105,000.[1]

The Complaint[2]

In his complaint form to the Office of the Arbiter for Financial Services ('OAFS'), the Complainant submitted that he was a victim of a cybercrime perpetrated by a fraudulent person(s) representing a fraudulent investment platform XPOKEN.com.

The said transfers consisted of 16 payment orders effected between 10 October 2022 and 20 July 2023 amounting to €97,500. The highest transfer was €20,000

[1] Page (p.) 3 - 4

[2] P. 1 - 7 with supporting documentation on P. 8 - 84.

on 03 April 2023 and then, there were 3 payments of €10,000 each, 1 payment of €9,000, 6 payments of €5,000 each, and 5 payments each for amounts less than €5,000.

From the Reply of Service Provider, it appears that before the fraud transfer started, the Complainant had a cash balance of €7,500 on his account with Crypto.com (trade and brand name of Foris) and this was also converted into digital assets and transferred out to fraudulent wallets so that the total loss amounts to €105,000.

In his complaint, he stated that:

"*On August 29, 2022 after seeing an advertisement on the social media platform Facebook, (the Complainant) discovered a platform called XPOKEN.com, which claimed to specialize in cryptocurrency investments.*

Seeking to explore online investment opportunities, (the Complainant) clicked on the link provided in the advertisement and created an account on the platform.

Immediately after creating his account, he was contacted by an alleged advisor from XPOKEN.com who encouraged him to invest €350 to begin making investment transactions on the platform.

Exhibit 1 – Proof of email exchanges between (the Complainant) and the alleged advisor of XPOKEN.com

Following daily phone conversations with the alleged advisor, (the Complainant) began making investment transactions, initially earning a profit of €1,000.

Convinced of the legitimacy of these operations (the Complainant) proceeded with financial commitments after being reassured by the alleged advisor from XPOKEN.com.

2.

To carry out transactions on the platform, (the Complainant) transferred funds from his two personal bank accounts to his account with XPOKEN.com.

The funds transferred by (the Complainant) were converted into USDT on the Crypto.com platform and subsequently transferred to the alleged trading platform XPOKEN.com.

Exhibit 2 – Proof of transfers made by (the Complainant) on the Crypto.com platform

Throughout these transactions, (the Complainant) concluded multiple financial agreements with XPOKEN.com, resulting in twelve consecutive transfers totalling €105,000 from August 29, 2022, to July 20, 2023.

Exhibit 3 – Financing contracts and asset agreements between (the Complainant) and XPOKEN.com

During this process, (the Complainant) was warned by the alleged advisor that he could lose all his funds deposited on the platform.

Subsequently, (the Complainant) felt compelled to secure loans from Caisse d'Epargne and Banque Populaire to cover the losses of his funds deposited on XPOKEN.com.

Later, the alleged advisor requested an additional investment of €92,000 from (the Complainant). When he refused, (the Complainant) was bombarded with incessant phone calls and emails from the advisor.

Overwhelmed by the situation, (the Complainant) realized he had been scammed and filed a complaint with the national gendarmerie on January 12, 2024.

Exhibit 4 – Extract from the official police report filed by (the Complainant)

On February 2, 2024, a bailiff's report documented the fraudulent transactions and movements of funds in (the Complainant's) bank accounts.

Exhibit 5 – Extract from the bailiff's report for (the Complainant).

As of today, (the Complainant's) financial loss amounts to €105,000.[3]

He maintains that Service Provider should have detected the irregularity of the transactions on his account and, therefore, held them responsible for the loss.

[3] P. 3 - 4

He claims that Foris should have protected him from sending his assets to the wallets controlled by the fraudsters and quoted various references to French law on this matter.[4]

Complainant denied he was guilty of negligence and explained that he had no intention of transferring his money for purposes other than investment and the Service Provider failed to note the unusual nature of the transfers and failed its duty of vigilance as it never contacted Complainant to flag the transaction and enquire its purpose[5]. He then quotes various transaction monitoring obligations that are principally related to obligations of banks under the EU Payments Directive commonly known as PSD 2.[6]

To his complaint, he attached documents in French language purporting to be

- Proof of transfers to Crypto.com.
- Exchanges with scammers from XPOKEN
- Extracts from official report filed with French police and bailiff related to this scam.

Complainant was invited to send English translation of documents considered important for his case as only translated documents could be included in the proceedings. No such translations were ever submitted.

Service Provider's reply

Having considered in its entirety the Service Provider's reply,[7]

Where the Service Provider provided a summary of the events which preceded the Complainant's formal complaint and explained and submitted the following:

1. *"Background*

    - *Foris DAX MT Limited (the '**Company'**) offers the following services: a crypto custodial wallet (the '**Wallet'**) and the purchase and sale of digital assets through the Wallet. Services are offered through the*

[4] P. 10 - 11
[5] P. 11
[6] DIRECTIVE (EU) 2015/2366 of 25 November 2015 on payment services in the internal market.
[7] P. 92 – 107 with attachments from p. 108 - 122.

*Crypto.com App (the '**App**'). The Wallet is only accessible through the App and the latter is only accessible via a mobile device.*

- *Our Company additionally offers a single-purpose wallet (the '**Cash Wallet**') (formerly referred to as the Crypto.com Fiat (EUR) Wallet), which allows customers to top up and withdraw fiat currencies from and to their personal bank account(s). This service is offered by the legal entity Foris MT Limited.*
- *(The Complainant), e-mail address xxxx@orange.fr, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 4 October 2022.*
- *The Company notes that in the submitted complaints file, the Complainant's representative has outlined the desired remedy as: (i) reimbursement for incurred financial losses*."[8]

The Service Provider then provided a timeline for the transactions of the Complainant's account with them for the above-mentioned inward transfer of Euro fiat currency. These funds were then converted to crypto assets and transferred out to an external wallet.

The Service Provider concluded that Complainant withdrew a total of USDT 105,265.49 from his wallet with Crypto.com over the period between 13.10.2022 and 20.07.2023 and these were transferred to three external non-hosted wallet addresses which later turned out to be fraudulent.

"Based on our investigation, the Company has concluded that we are unable to honor the Complainant's refund request based on the fact that the reported transfers were made by the Complainant himself.

While we sympathize with the Complainant and recognize that he may have been misled or induced into transferring funds to an alleged fraudster, it is important to note that these transfers were made solely at the Complainant's request. We must also emphasize that the addresses the funds were transferred to, do not belong to the Company and as such, any due diligence of the

[8] P. 24

ownership of these addresses falls under the responsibilities of the provider of said wallets.

Unfortunately, Crypto.com cannot revoke any virtual asset withdrawals because blockchain transactions are fast and immutable.

The Complainant is solely responsible for the security and authenticity of all instructions submitted through his Wallet as outlined in the Foris DAX MT Limited Terms of Use.

Please see the relevant section of the Terms of Use for your reference:

QUOTE

6.2

Without prejudice to the foregoing and any other terms in these Terms, we assume that any and all instructions received from your Enabled Device have been made by the rightful owner. You are solely responsible and liable for keeping your enabled Device safe and maintaining adequate security and control of your login and authentication details (including, but not limited to, your username, and password), and shall likewise be solely responsible for any access to and use of the Crypto.com App and the Services through your Enabled Device, notwithstanding that such access and/or use may have been effected without your knowledge, authority or consent. We will not be liable to you for any loss or damage resulting from such access and/or use.

…

7.2 Digital Asset Transfers

…

(b) Crypto.com processes all Digital Asset Transfers according to the instructions received from you and does not guarantee the identity of any recipient. You should verify all transaction information prior to submitting instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed by Crypto.com unless Crypto.com decides at its sole discretion that the transaction should be cancelled or reversed and is technically capable of such cancellation or reversal. You acknowledge that you

are responsible for ensuring the accuracy of any instructions submitted to Crypto.com and that any errors may result in the irreversible loss of your Digital Asset.

…

UNQUOTE

In summary, it seems conceivable that the Complainant has been the victim of an alleged scam. However, due to the nature of the external wallet and the fact that it is not hosted or operated by Foris DAX MT, we can neither confirm nor deny this.

Whilst we fully empathize with (the Complainant) in this regard, it cannot be overlooked that he had willingly, transferred his virtual asset holdings from his Crypto.com Wallet to external wallet addresses which he nominated.

As outlined above in the Foris DAX MT Limited Terms of Use, the Complainant is solely responsible for the security and authenticity of all instructions submitted through the Crypto.com App and, as such, the Company cannot accept liability for the veracity of any third party or for the instructions received from the Complainant themselves."[9]

Hearings

For the first hearing on 17 June 2025. both the Complainant and his legal representative failed to make presence.

At the second hearing of 22 September 2025, only the legal representative was present and the Complainant's absence was simply explained as *'preferred not to come'*. [10]

This raised objections from the Service Provider who in the absence of possibility to cross-examine the evidence submitted by Complainant claimed that such evidence should not be considered.

The Arbiter ruled that in the absence of Complainant making himself available for cross-examination, he is taking a clear position that the payments and

[9] P. 105 - 107
[10] P. 124

transfers complained of were executed with the full authority of the Complainant and the Service Provider need only defend themselves from the claim that through their monitoring systems, they should have stopped the transfers to external wallets controlled by the fraudsters as there were clear signs of fraud.

Complainant's lawyers assented to such ruling and confirmed that the payment was made with full authority of the Complainant.[11]

The Complainant's representative merely repeated what was already stated in the Complaint as registered.

The Arbiter explained that as Complainant has accepted that he had personally authorised the transfers subject of this complaint, the issue of not being at fault because he did not disclose his secret credentials is irrelevant. The relevant issue is whether the Service Provider could or should have done anything, according to law and regulations, to identify the fraud and stop the payments despite their being fully authorised.

At the hearing, the Arbiter reminded the Complainant's representative to file an English translation for the report in French attached to the complaint.

The Service Provider explained that they cannot cross examine the legal representative and protested the absence of the Complainant.

They also tried to raise prescription issues related to Article 21 (1)(c) of CAP. 555 but the Arbiter refused to consider the prescription issue as this should have been raised in the first written submission in terms of Article 22(3)(c) of CAP. 555.

Service Provider asked if the Complainant had started any proceedings against his home banks for not alerting him to fraud risks. The legal representative of Complainant informed that she had no such information available.

At the last hearing held on 25 November 2025, the Complainant again failed to make presence. His legal representative informed that protests/claims against the home banks were made on 27 December 2024 alongside the protest to Foris

[11] P. 125

but had no clear answers about the outcome. She made reference to referral to mediation.

The evidence of the Service Provider was presented by Ms Pema Fung who stated:

"***Without repeating what has already been said in our reply, the complainant became a customer and user of the service provider on the 4th of October in 2022. The disputed transactions in question relate to the withdrawals of cryptocurrency, which were purchased on the Crypto.com app to 3 different external wallet addresses between 13th of October 2022 to 20th July 2023.***

These wallet addresses are what we call non-custodial addresses which means they are not serviced by Crypto.com or the service provider, or as identified from the data on the blockchain, they are not provided by service providers of similar sphere.

From the evidence at hand and the agreement of the complainant's legal representative, these transactions were fully authorized by the complainant.

At the time of the withdrawals, none of the address wallets in question, were subject to any warnings from our own internal investigations or any third-party transaction monitoring tools that we use.

I can confirm that we do not have any affiliation with the platform XPOKEN.

I say that there was nothing on our own controls, as well as the controls of our third-party employed tools to indicate that there was any malicious or scam activity involved in these cases at the time of these transactions.

We were also not communicated with or brought to our attention by the complainant any concerns with these transactions until they had been completed.

Therefore, insofar as the transactions have been completed to the full satisfaction of what we were asked to execute on behalf of the complainant, we would say that we have no responsibility with regard to these disputed transactions.

In our reply (and this was also mentioned in the transcript on page 126), I state that we received the complaint on the 1st of April 2024, even though the

complainant says that this was sent on the 24th of December 2024 and 26th of December 2024.

It is being said that in our reply of 11 February 2025, (page 14 of the process), we said that we never received the complaint on the previous dates and only received it on 26 December 2024.

"We refer to your letter dated 1 April 2024 and 24 December 2024 which were both received by us on 26 December 2024. We do not have any record of receiving your letter dated 1 April 2024."

I say that as far as the legal team is concerned, the first correspondence we received was dated 26 December 2024."[12]

The representative of the Complainant declined an offer to cross-examine.

Final submissions

In their final submissions, the parties largely restated what was already presented in the proceedings.

Having heard the parties

Having seen all the documents

Considers

Applicable Regulatory Framework

Foris DAX was, at the time of the events leading to this complaint, the holder of a Class 3 VFAA licence granted by the Malta Financial Services Authority ('MFSA') under the Virtual Financial Assets Act, 2018 ('VFAA').

Apart from the relevant provisions under the VFAA, and the *Virtual Financial Assets Regulations, 2018 (L.N. 357 of 2018)* issued under the same act, Foris DAX was also subject to the rules outlined in the Virtual Financial Assets Rulebook ('the VFA Rulebook') issued by the MFSA. The said rulebook complements the VFAA by detailing *inter alia* ongoing obligations applicable for VFA Service Providers.

[12] P. 129 - 130

Chapter 3 of the VFA Rulebook specifically includes the rules applicable for VFA Service Providers which such providers must adhere to.

The Arbiter further notes that in the year 2020, the MFSA has also issued a *'harmonised baseline guidance on Technology Arrangements'*[13] applicable to its licence holders (including under the Virtual Financial Assets) titled *'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'* ('the Guidance').

Further Considerations

Having considered the particular circumstances of the case including the submissions made and evidence provided, the Arbiter considers that at no stage has the Complainant raised any doubt as to his having authenticated the transactions personally.

The Arbiter further considers various factors, including the nature of the complaint, activities involved, and the alleged shortfalls as further detailed below:

- The Complaint involves a series of payments made by the Complainant from his account held with Foris DAX, to unknown external wallets.

  The Arbiter considers that no adequate and sufficient evidence has however emerged to substantiate the claim that the Service Provider could have itself prevented or stopped the transaction. This is also given the nature of the transactions which involved crypto assets, the type of service provided, and other reasons as outlined below.

- The exchange of fiat currency into crypto and withdrawals from one's crypto account, including withdrawals to an external wallet is part of the typical services provided to millions of users by operators in the crypto field such as the Service Provider.

- Furthermore, it has not been demonstrated nor emerged that the alleged fraudster, to whom the payment was made by the Complainant, was

[13] Guidance 1.1.2, Title 1, *'Scope and Application' of the 'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'*.

another *Crypto.com* App user and, thus, a client of the Service Provider in the first place. The transfer was rather indicated to have been done to an *'external wallet'* and hence the Service Provider had no information about the third party to whom the Complainant was transferring his crypto.

- The Complainant seems to have only contacted the Service Provider well after the last of the disputed transactions was already executed and finalised.[14]

Once finalised, the crypto cannot be cancelled or reversed as specified in the Service Provider's Terms and Conditions of Use (and as typically indicated on various other internet sites).[15]

Once a transaction is complete, and accordingly is not in a pending state, the crypto transaction cannot be cancelled or reversed by the Service Provider as provided for and warned in the Terms and Conditions of Foris DAX.

As indicated by the Service Provider, Clause 7.2(b) of its Terms and Conditions regarding the use of the Crypto.com App Services specifies that:

'Crypto.com processes all Digital Asset Transfers according to the Instructions received from you and does not guarantee the identity of any recipient. You should verify all transaction information prior to submitting Instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed …'.[16]

Based on the facts presented during the case, the Arbiter could not conclude that the Service Provider failed to adhere to any specific obligation, or any specific regulatory requirements applicable to it, nor did he find any infringement of the Terms and Conditions applicable in respect to the service offered.

In arriving at his decision, the Arbiter considered the following aspects:

[14] Crypto transactions may be processed and completed within a few minutes or hours (as indicated on various websites following a general search on the internet).
[15] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency
[16] P. 106

i. AML/CFT Framework

Further to the Prevention of Money Laundering Act (Cap. 373) and Prevention of Money Laundering and Funding of Terrorism Regulations ('PMLFTR'), the Financial Intelligence Analysis Unit (FIAU) issued Implementing Procedures including on the *'Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector'*.

These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[17] Section 2.3 of these Implementing Procedures detail the monitoring and transaction records obligations of VFA licensed entities.

It is noted that the VFA Act, mainly imposes transaction monitoring obligations on the Service Provider for the proper execution of their duties for Anti Money Laundering ('AML') and Combating of Financing of Terrorism ('CFT') obligations in terms of the local AML and CFT legislative framework.

Failures of the Service Provider in respect of AML/CFT are not in the remit of the OAFS and should be addressed to the FIAU. In the course of these procedures, no such failure was indeed alleged. The Arbiter shall accordingly not consider compliance or otherwise with AML/CFT obligations in this case.

ii. MiCA and the Travel Rule

As to the identification of the recipient of the funds, it is noted that MiCA[18] and Travel Rule[19] obligations which entered into force in 2025 and which give more protection to consumers by having more transparency of the owners of the recipient wallets, were not applicable at the time of the events covered in this Complaint which happened in 2023.

[17] Page 6 of the FIAU's Implementing Procedures on the *'Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector'*

[18] EU Directive 2023/1114 on markets in crypto assets https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:32023R1114

[19] EU Directive 2023/1113 https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32023R1113&qid=1740401464257&rid=1 and EBA Guidelines on Travel Rule https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf

The Arbiter shall thus not consider the MiCA provisions and Travel Rule obligations for the purposes of this Complaint.

iii. Other - Technical Note

A Technical Note (issued in 2025) with guidance on complaints related to pig butchering was recently published by the Arbiter. In respect of VFA licensees the Technical Note states as follows:

> *"Virtual Financial Assets Service Providers (VASPs)*
>
> *VASPs should be aware that with the coming into force of Regulation (EU) 2023/1113 and the Travel Rule Guidelines[20] 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),[21] 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.[22]*

The Arbiter will not apply the provisions of the Technical Notes retroactively.

---

[20] *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

[21] Such as Case ASF 158/2021

[22] Such as Case ASF 069/2024

Hence, for the avoidance of any doubt, the said Technical Note is not applicable to the case in question.

iv. Duty of Care and Fiduciary Obligations

It is noted that Article 27 of the VFA Act states:

> *"27. (1) Licence holders shall act honestly, fairly and professionally and shall comply with the requirements laid down in this Act and any regulations made and rules issued thereunder, as well as with other legal and regulatory requirements as may be applicable.*
>
> ***(2) A licence holder shall be subject to fiduciary obligations as established in the Civil Code (CAP 16) in so far as applicable**."*[23]

Article 1124A (1)(a) of the Civil Code (Chapter 16 of the Laws of Malta), in turn further provides the following:

> *"1124A. (1) **Fiduciary obligations arise in virtue of law, contract, quasi-contract**, unilateral declarations including wills, trusts, **assumption of office or behaviour whenever a person** (the ''fiduciary'') –*
>
> *(a) **owes a duty to protect the interests of another person and it shall be presumed that such an obligation where a fiduciary acts in or occupies a position of trust is in favour of another person**;…"*[24]

It is further to be pointed out that one of the High Level Principles outlined in Section 2, Title 1 *'General Scope and High Level Principles'* Chapter 3, Virtual Financial Assets Rules for VFA Service Providers of the VFA Rulebook, that applied to the Service Provider at the time of the disputed transactions in 2022, provides that:

> *"R3-1.2.1 VFA Service Providers shall act in an ethical manner taking into consideration the best interests of their clients and the integrity of Malta's financial system."*

[23] Emphasis added by the Arbiter
[24] Emphasis added by the Arbiter

It is also noted that Legal Notice 357 of 2018, Virtual Financial Assets Regulations, 2018 issued under the VFA Act, furthermore, outlined various provisions relevant and applicable to the Service Provider at the time. Article 14 (1) and (7) of the said Regulations, in particular, which dealt with the *'Functions and duties of the subject person'* provided the following:

> *"14. (1) A subject person having the control of assets belonging to a client shall safeguard such assets and the interest of the client therein.*
>
> *…*
>
> *(7) The subject person shall make appropriate arrangements for the protection of clients' assets held under control and shall ensure that such assets are placed under adequate systems to safeguard such assets from damage, misappropriation or other loss and which permit the delivery of such assets only in accordance with the terms and conditions of the agreement entered into with the client."*

The Arbiter is of the view that for the general fiduciary obligations to apply in the context of the VFA ACT, there must be something which is truly out of the ordinary and which should really act in a conspicuous manner as an out of norm transaction which triggers the application of such general fiduciary duties.

In the particular circumstances of this case, there is nothing which is out of the ordinary to a degree which should have triggered the application of the fiduciary duties of the Service Provider. The complaint involved 16 payments spread over 9 months with a regular pattern and a highest payment of €20,000 which was not out of line with the pattern of payments in a way that should have raised suspicion of fraud. There were no payment patterns which could have given rise to reasonable suspicion of fraud, and Complainant was clearly warned, as was prudent, to ensure that he knows and has confidence in the beneficiaries of the external wallet.

Decision

It is probable that the Complainant has, unfortunately, fallen victim of a scam done by a third party and no evidence resulted that this third party is in any way related to the Service Provider.

The Arbiter notes that the crypto business is a relatively new area with no *harmonised regulation* existing at the time of the disputed transactions. An EU regulatory framework was only recently implemented effective for the first time in this field in 2025.[25]

Whilst this area of business had remained unregulated in certain jurisdictions, other jurisdictions, like Malta, chose to regulate this field in the meantime and subject it to a home-grown national regulatory regime. While such regimes offer a certain amount of security to the consumer, since they are still relatively in their infancy, may not necessarily reflect the same standards and protections applicable in other sectors of the financial services industry which have long been regulated.

In fact, the Arbiter notes that in his complaint, the Complainant refers to provisions of the PSD 2,[26] as translated into French legislation, which whilst applying to banks are not applicable to VFA licensees.

A person who chooses to venture into the area of crypto which, itself, is typically a highly speculative and risky market, needs to also be highly conscious of the potential lack of, or lesser, consumer protection measures applicable to this area of business, as compared to those found and expected in other established sectors of the financial services industry. EU regulatory bodies have issued various warnings to this effect over the past years.[27]

---

[25] Provisional agreement has been reached on the EU's Markets in Crypto-Assets Regulation (MiCA) only in June 2022 - https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/
MiCA entered into force in 2025 – https://www.financemagnates.com/cryptocurrency/can-mica-take-europe-to-the-crypto-promised-land/

[26] EU Directive 2015 - 2366

[27] https://www.eiopa.europa.eu/document-library/othis-documents/crypto-assets-esas-remind-consumers-about-risks_en
https://www.esma.europa.eu/sites/default/files/library/esa_2022_15_joint_esas_warning_on_crypto-assets.pdf

The Arbiter must also consider that the obligations of fiduciary duty and transaction monitoring apply more forcefully to licensed banks than they apply to CASPs/VFA agents. Banks have a much longer relationship with their clients, and they have the data to spot unusual transactions and suspect fraud.

On the other hand, customer's relationship with a VFA is short without much historical data to enable early spotting of unusual patterns of payments.

Banks can only avoid, under the provisions of PSD 2, to reimburse fraud payments even if authenticated and authorised by their client if the client has shown gross negligence in the process.

In terms of preamble 71 of the said PSD2,[28] the PSU (Complainant) shall be responsible for payment of any unauthorised payment transaction only up to a limit of €50, unless the PSU has acted fraudulently or with gross negligence.

In the absence of gross negligence, there could well be an obligation on the part of the home bank to make quasi-total refunds to their client (Complainant). The banks' obligations for effective transaction monitoring are direct and specific under the EU Directive PSD 2. On the other hand, the transaction monitoring obligations on CASP/VFA result only from general fiduciary duties and are less direct and forceful than those applicable to banks.

[28]Preamble 71 of PSD 2 (**DIRECTIVE (EU) 2015/2366)** states:
In the case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of that transaction to the payer. However, where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payment service user and where that suspicion is based on objective grounds which are communicated to the relevant national authority, the payment service provider should be able to conduct, within a reasonable time, an investigation before refunding the payer. In order to protect the payer from any disadvantages, the credit value date of the refund should not be later than the date when the amount has been debited. In order to provide an incentive for the payment service user to notify, without undue delay, the payment service provider of any theft or loss of a payment instrument and thus to reduce the risk of unauthorised payment transactions, the user should be liable only for a very limited amount**, unless the payment service user has acted fraudulently or with gross negligence**. In that context, an amount of EUR 50 seems to be adequate in order to ensure a harmonised and high-level user protection within the Union. There should be no liability where the payer is not in a position to become aware of the loss, theft or misappropriation of the payment instrument. Moreover, once users have notified a payment service provider that their payment instrument may have been compromised, payment service users should not be required to cover any further losses stemming from unauthorised use of that instrument. This Directive should be without prejudice to payment service providers' responsibility for technical security of their own products. (emphasis added by Arbiter)

If reimbursement of losses is denied by the home bank on the basis of gross negligence on the part of the Complainant, the same gross negligence would exempt Foris from being a clear direct cause of his claimed losses.

In spite of the passage of time (last payment was effected on 20.07.2023), no evidence has been provided that a proper claim was made against the remitter French banks.[29]

The legal representative of the Complainant gave rather scant information about the claim against the home banks only stating it has been referred to mediation (presumably after being refused by the bank).[30] This gives rise to suspicion of forum shopping after failure of getting any recoveries from Caisse d'Epargne and Banque Populaire, possibly due to gross negligence on the part of Complainant.

The Arbiter sympathises with the Complainant for the ordeal he may have suffered as a victim of a scam but, in the particular circumstances of this case, he cannot accept the Complainant's request for compensation as he has failed to provide any evidence that Service Provider has failed in their regulatory and fiduciary obligations.

Consequently, this complaint is not upheld and no compensation is being ordered.

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

Alfred Mifsud
Arbiter for Financial Services

[29] P. 128
[30] P. 133 In final submissions, they confirm rejection of the claim by one of the French Banks.

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. Personal details of the Complainant(s) will be anonymised in terms of article 11(1)(f) of the Act.