Before the Arbiter for Financial Services

Case ASF 045/2025

DS ('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C88392)

('Foris' or 'the 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 account with Crédit Agricole bank in France to his crypto account with Service Provider) to a fraudulent platform, has caused her a financial loss for which she is seeking compensation of €31,999[1].

The Complaint[2]

In her complaint form to the Office of the Arbiter for Financial Services ('OAFS'), the Complainant submitted that she was a victim of a cybercrime perpetrated by a fraudulent investment platform 'Futur BTC' through *Crypto.com* whose misconduct allowed the fraudster operating the fraudulent platform to steal her money.

[1] Pages (p.). 4

[2] P. 1 - 7 with supporting documentation on P. 8 - 70.

She stated that she found the platform 'Futur BTC' on the internet and saw it was not subject to any warning on the list of AMF (French Financial Market Authority) and she could see they there were positive online reviews on their reliability. She started with a small investment of just €179 and was then contacted by an assistant urging her to activate her investment account.

A certain Mr Steafan introduced himself as her account manager and was particularly friendly and attentive to her needs. He informed her that he was licensed on the FINMA register.

Complainant started see good returns on her investments and she was encouraged to invest more. At one stage, he suggested an investment of fifty thousand euros to reach Gold status.

It results that the following payments were made on the platform through Crypto.com:

Date	**Amount €**	**Reference**
15.05.2023	10	p. 76; 28
17.05.023	2,500	p. 76; 28
19.05.2023	2,500	p. 77; 28
22.05.2023	2,500	p. 78; 28
22.05.2023	2,320	p. 78; 28
23.05.2023	2,500	p. 79; 28
24.05.2023	12,500	p. 80; 28
25.05.2023	2,000	p. 81; 28
22.06.2023	5,000	p. 82; 31
TOTAL	**31,810**	

Note: Total evidenced payment is €31,800 whilst claim for compensation is €31,999. The latter possibly includes the first investment of €179 which does not seem to have been handled by Crytpo.com.

The Arbiter is considering that the claim is for €31,810.

On 25 May 2023, Steafan objected to her plan to withdraw her investments and guided her with Anydesk App how to conduct the withdrawal, but Complainant panicked when she saw her investments disappearing. Steafan blamed her early wish to withdraw for the disappearance and convinced her to deposit another €2,000 *"to create leverage"*[3].

On 21 June 2023, a new adviser named Jean Pierre told her that her account turned positive again and was showing a profit of €88,900 and needed a tax payment of 10% €8,900 to facilitate withdrawal. On 22 June, Complainant ordered all her positions closed not to risk losing her gains and paid the last €5,000 promising to pay the difference once she recovers her investment and profits. Obviously, she never recovered anything and on 02 August 2023, convinced she had been scammed, she filed a bailiff report.

In her complaint, she presented evidence of exchanged correspondence with Futur BTC explaining the investment[4].

However, as the Arbiter has no competence as regards Futur BTC, this documentation is quite irrelevant to this complaint as Foris was not a party to such exchanges and had no access to such knowledge at the time when the transfers complained of were being executed.

She maintained that Service Provider should have detected the irregularity of the transactions on her account and should at the very least have questioned her and informed her of the potential suspicious nature of the transactions[5].

It was claimed that Foris should have protected Complainant from sending her assets to the wallets controlled by the fraudsters and quoted various references to French law on this matter.[6]

Complainant denied she was guilty of negligence and explained that she had no intention of transferring her money for purposes other than investment and Service Provider (whom she addresses as Bank/neobank) failed to note the

[3] P. 3
[4] P. 17 - 25
[5] P. 10
[6] P. 10 -12

unusual nature of the transfers.[7] She then quotes various transaction monitoring obligations related to banks and finally concludes as follows:

> *"In this case, (Complainant) made no mistake. Indeed, she was quick to contact her adviser to obtain further information about her situation when she became aware that the entire procedure was fraudulent.*
>
> *Furthermore, (Complainant) did not disclose any personal data to third parties.*
>
> *Consequently, (Service Provider) must return the funds to the client as she was not at fault".*[8]

Service Provider's reply

Having considered, in its entirety, the Service Provider's reply[9]

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

> *"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 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 xxxxx@gmail.com, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 3 May 2023.*

[7] P. 11
[8] P. 12
[9] P. 75 – 84 with attachments from p. 85 - 96.

- *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*."[10]

The Service Provider then provided a timeline for the transactions of the Complainant's account with them. These consisted of the above-listed 9 inward transfers of Euro fiat currency collectively amounting to €31,810. These funds were then converted to crypto assets (BTC) and the transferred through 7 transactions totalling BTC 1.22471785 to an external wallet ending with reference … 2xl49.[11]

"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 herself

While we sympathize with the Complainant and recognize that she 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 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 her 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:

[10] P. 75
[11] P. 82

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 she had willingly, transferred her virtual asset holdings from her Crypto.com Wallet to external wallet addresses which she 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."[12]

Hearings

During the hearings, the Complainant failed to make presence and was represented by her French counsel who largely restated the contents of the filed complaint.

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 herself available for cross-examination, he is taking a clear position that the payments and 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 whilst Service Provider wished to register the following statement:

"On behalf of the service provider, the absence of the complainant naturally renders cross-examination impossible and deprives the service provider of its fundamental right to test the complainant's evidence and the content of her complaint.

[12] P. 82 - 84

In the proceedings which are adversarial as the one we have today, this opportunity to cross-examine is not a mere formality. It is a core aspect of natural justice and this failure of not having a cross-examination, undermines the veracity and the value of the claim.

Therefore, the service provider contests that proceedings should continue."[13]

The Arbiter explained that as Complainant has accepted that she had personally authorised the transfers subject of this complaint[14], the issue of not being at fault because she did not disclose her 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 in spite of their being fully authorised.

At the hearing, the Arbiter requested the Complainant's representative to file a translated copy of the fraud report made to the French Authorities.

Complainant's representative also confirmed that they sent a letter of complaint to Crédit Agricole but no reply has yet been received, and no proceedings have been started.[15]

A translated copy of a report dated 30 September 2025 filed with the French Public Prosector was submitted.[16]

The Arbiter notes that this report is separate from the first report to the Bailiff dated 02 August 2023[17] of which an untranslated copy was annexed to the complaint. As the latter was not properly translated, the Arbiter relies on the Public Prosecutor document which was filed after the first hearing held on 22 September 2025.

During the second hearing (where complainant again failed to make presence) held on 25 November 2025, the Service Provider's representative, Ms Pema Fund stated:

[13] P. 98
[14] Ibid.
[15] P. 99
[16] P. 101 - 109
[17] P. 36 - 70

"The complainant became a client of the service provider on the 3rd of May 2023.

The disputed transactions in question relate to the withdrawal of cryptocurrency, which was purchased on the Crypto.com app, to one external wallet address between the dates of 18th of May to 22nd of June 2023. The wallet address is what we call a non-custodial address, and this means they are not serviced by Crypto.com or, as identified from data on the blockchain, they are not provided by service providers of a similar sphere.

From the evidence at hand and the agreement of the complainant's legal representative, these transactions were fully authorised by the complainant. At the time of the withdrawal, 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. That is to say, there was nothing in our own controls or any third party employed tools to indicate that there was any malicious or scam activity involved in these cases at the time of the transactions.

Also, we were not communicated with or brought to the attention by the complainant either regarding any concerns with these transactions until these transactions had already 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 bear no responsibility with regards to the disputed transactions.

And, in this case, being May/June 2023, it is also the case where the warnings were not part of the system."[18]

There was no cross-examination of Ms Fung's evidence by the legal representative of the Complainant.

Final Submissions

In their final submissions, the parties basically repeated what had already emerged in the complaint, the reply and the hearing proceedings.

[18] P. 112

No additional documents were submitted by Foris regarding warnings given to clients every time they whitelist a wallet address and before each transfer is effected to an external wallet.

Having heard the parties

Having seen all the documents

Considers

In failing to give proper evidence before the Arbiter and denying the Service Provider their right for a proper cross-examination of the case made in her complaint, the Complainant has substantially prejudiced her case.

As the identity of the beneficial owners of the external wallets' recipients of the claimed fraudulent payments cannot be established, it was necessary to hear an emphatic negation from the Complainant that she was a party to such wallets.

Such emphatic negation was only forthcoming from the side of the Service Provider.

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.

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'*[19] 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 there is no sufficient and adequate basis on which he can uphold the Complainant's request for the reimbursement by the Service Provider of the sum the Complainant herself transferred to an external wallet from her crypto account.

At no stage has the Complainant raised any doubt as to her having authenticated the transactions personally.

This is particularly so when taking into consideration 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 her account held with Foris DAX, to an unknown external wallet.

  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, in its own right, part of the typical services provided to millions of users by operators in the crypto field such as the Service Provider.

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

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

- The Complainant seems to have only contacted the Service Provider on 30 September 2023,[20] more than 3 months after the last of the disputed transactions was already executed and finalised.[21]

  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).[22]

  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 …'.[23]

  On the basis of 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

[20] P. 8
[21] 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).
[22] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency
[23] P. 83

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:

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'*.[24]

These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[25] 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[26] and Travel Rule[27] obligations which entered into force in 2025 and which give more

[24] https://fiaumalta.org/app/uploads/2020/09/20200918_IPsII_VFAs.pdf

[25] 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'*

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

[27] 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

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 2024.

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[28] 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),[29] 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*

[28] *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

[29] Such as Case ASF 158/2021

empty the bank accounts of retail customers and disappear such funds in the complex web of blockchain anonymous transactions.[30]

***Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications**."*[31]

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

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**."*[32]

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****;…"*[33]

[30] Such as Case ASF 069/2024
[31] Emphasis added by the Arbiter
[32] Emphasis added by the Arbiter
[33] Emphasis added by the Arbiter

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."*

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.

No such out of norm event can be claimed during the short period of just over one month when the fraudulent transfers were happening in relatively consistent quantity values in funds transferred from Complainant's account with her French Bank.

The Arbiter when considering the particular circumstances of this case, considers that the Service Provider did not breach, in terms of the provisions outlined in this decision, the duty of care and fiduciary obligations towards its customer, the Complainant.

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

Ultimately, the Arbiter does not consider that in the case in question, there is any clear and satisfactory evidence that has been brought forward, and/or emerged, during the proceedings of the case which could adequately corroborate that the Service Provider failed in any of the applicable obligations, contractually and/or arising from the VFA regulatory regime applicable in respect of its business.

The Arbiter notes that the crypto business is a relatively new area with no *harmonised regulation* existed 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.[34]

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 her complaint, the Complainant refers to provisions of the PSD 2,[35] as translated into French legislation, which whilst

[34] 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/

[35] EU Directive 2015 - 2366

applying to banks are not applicable to VFA licensees. She also often wrongly addresses Foris as a bank/neo bank, which clearly, they are not.

The Arbiter was informed that similar claims for compensation were made on Complainant's French Bank on the basis that they had an obligation to intervene and stop Complainant from transferring her funds to a crypto exchange, given the much longer relationship between Complainant and her Bank permitting them to view in better context the claimed abnormality of such payments.

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.[36]

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[37], 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.

---

[36] 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

[37] 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

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.

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 22.06.2023), no evidence has been provided that a proper claim was made against the remitter French bank. The legal representative of the Complainant gave rather scant information about the claim, if any, done against the home bank. This gives rise to suspicion of forum shopping after failure of getting any recoveries from Crédit Agricole possibly due to gross negligence on the part of Complainant.

Decision

The Arbiter sympathises with the Complainant for the ordeal she 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 for the reasons amply mentioned.

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)

The losses she suffered were basically caused by her gross negligence in not conducting proper checks on Futur BTC prior to investing, and by greed searching for quick and easy profits.[38]

The Arbiter is accordingly rejecting the Complaint.

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

However, the Arbiter warns that for new complaints registered after September 2025, in cases where the Complainants fail to attend hearings to defend their complaint without valid reasons, they will be obliged to settle the fees of the respondent service providers.

Alfred Mifsud
Arbiter for Financial Services

Information Note related to the Arbiter's decision

Right of Appeal

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

Any requests for clarification of the award or requests to correct any errors in computation or clerical or typographical or similar errors requested in terms of article 26(4) of the Act, are to be filed with the Arbiter, with a copy to the other

[38] p. 4, "*… had €88,900 in winnings*."

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.