Before the Arbiter for Financial Services

Case ASF 214/2024

UA ('Complainant')

Vs

Foris MT Limited

Reg. No. C 90348

('Service Provider' or 'Foris')

Sitting of 12 September 2025

This case concerns an unmet claim for refund of €804.95 representing 8 transactions[1] claimed fraudulent which were charged to the Complainant's prepaid VISA card without his authority.

The Complainant maintains that his card was linked without his authority to Apple Pay on an Apple mobile device, whereas he has no such Apple device and has never requested or authorised such linking.

In his Complaint,[2] he maintains that:

1. Article 73 of PSD 2 (EU Payments Services Directive 2015/2366)[3] mandates a swift refund of unauthorised transactions in the absence of strong authentication.

2. Foris do not meet statutory requirements for SCA (Strong Customer Authentication) in terms of the said Article 73 of PSD2.[4]

[1] Page (p.) 15
[2] P. 1 - 7 and attachments p. 8 - 19
[3] Article 73 is reproduced in an annex to this decision

[4] SCA is in fact defined in Article 4 (30) of PSD 2 as 'strong customer authentication' means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in

3. Foris have inadequate fraud detection systems which would have flagged the payments as suspicious.

4. There was insufficient communication on Foris part to inform about the registration of his card on Apple Pay.

He considers that these failures on the part of the Service Provider render them responsible to make a full refund for the fraudulent charges to his account. He also requests additional compensation of €150 for the inconvenience and time spent trying to resolve this matter.

He further explained that on 28/10/2024, he attempted to make a purchase on a website that turned out to be fraudulent. He further admitted that the site *"used the OTP (one time password) code received by SMS to add my card to Apple Pay"*.[5]

He added that after the fraudulent payments of 05/11/2024, he blocked his card on the App of Crypto.com (brand name of Foris) and filed a complaint with the French Gendarmerie.

Reply of Service Provider

In their reply,[6] Foris stated that the Complainant had been their customer since 13 May 2021.

The 8 transactions subject of this complaint were deemed not qualifying for a chargeback as they were executed with a VISA card which was successfully uploaded on to Apple Pay through an OTP sent by SMS to his registered mobile number.

"The SMS/OTP confirmation was sent to and authorised from the user's personal mobile device, thereby confirming the user's consent and authorisation for integrating the card with Apple Pay and subsequently approving the transactions."[7]

that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data

[5] p. 8

[6] p. 25 – 28 and attachment p. 29

[7] P. 27

They concluded that as the transactions were validated through a secure authentication method, these transactions were properly authorised and are unable to consider the transactions as unauthorised or fraudulent.

Hearings

During the first hearing held on 03 April 2024, the Complainant confirmed:

1. The transactions subject of his complaint were dated 05 November 2024 but were shown on his statement on the next day.
2. He blocked the VISA card on 06 November 2024 when he became aware of the transactions.
3. He received communication about these transactions on his Crypto.com App on his Android phone, but he received no SMS notification of such purchases.
4. His card was linked to Google Pay and he never had problems with Google Pay.
5. He confirmed receiving a notification from Crypto.com with an OTP to link his card with Apple Pay but *"I never entered this code on the website".*[8] He also confirmed having received notification on 28 October 2024 of his card being uploaded on Apple Pay.[9]

There was controversy during the evidence about what exactly was disclosed on the merchant website when he pressed the link, so this evidence is reproduced verbatim hereunder:

"The Arbiter intervenes to say that he had asked this question, whether I put in the code on my website or whether I disclosed it to someone else and I answered 'No, I didn't'. before the page went blank and I said yes.

Now Dr Bencini asked me whether I put that code before the page went blank and I said, 'Yes'.

Asked by the Arbiter which one is the answer, I say that I typed the date and CVC of my Visa card, but I could not write the OTP code.

[8] P. 34
[9] *Ibid*.

I say, yes. On this website I input my Visa card, the expiry date of my Visa card and the three-digit CVC but I did not input the code that was sent to me to link it to Apple Pay. I could not do that.

I say that when I input these things, the website went blank.

Asked whether this was on the 28th of October, I say, yes.

Asked whether anything happened before the 5th of November, I say, nothing.

Asked whether I tried to get it back into that website on the 29th, on the 30th or on the 1st November or whatever, I say, no, nothing. And I don't have a transaction for that. I think the payment doesn't work.

Asked whether it is correct what I said that I do not have an iPhone, I say that is correct.

But it is being said that on the 28th of October 2024, I received an SMS notification from Crypto.com providing me with registration for Apple Pay and an OTP.

I say, yes, but I did not see that.

Asked when I first noticed this SMS, I say when you answer me, you, Mr UA, are registered your card in Apple Pay. I discovered this SMS when you replied to my complaint.

It is being said that I did not check the SMS when I received it from Crypto.com.

I say, no. I did not see this SMS before.

Asked whether I normally check notifications I receive from Crypto.com, I say, no I do not read SMSes.

It is being said that Crypto.com informed me of this notification and of subsequent transactions, but I do not check my SMS notifications.

Asked whether this is correct, I say I don't know.

Asked how I went to that website on the 28th of October when I wanted to purchase things, I say with my phone.

Asked whether I typed in the website address in the browser bar or whether I clicked on a link from an advertisement, I say I made a Google search.

So, it is being said that I clicked on a link from Google Search.

I say, yes, and the website is https. I checked that before.

I say, yes, it was a link from Google Search for the website.

Asked whether I purchased anything from this website before, I say, never. I did not know of this website before.

The Arbiter requests the service provider to present a copy of all SMSes which were exchanged between Crypto.com and the complainant on the registered mobile number

Ms Pema Fung, for the service provider, says that she has to check with their back end because some of the messages could have been sent by Visa.

The Arbiter states that they need to understand who took the initiative to send these SMSes as Crypto.com does not send an SMS to someone to link his card to Apple Pay unless somebody makes this request.

To this end, the Arbiter needs to know who made the request and what was sent by Crypto.com and on which number, with the proof that that number is the number which Mr UA registered on his account because if that happened, then the mystery of how that number could have been used by somebody who did not get that number to link his card to Apple Pay has to be solved.

The Arbiter requests that a representative from the technical side of Crypto.com be present at the next hearing to explain what occurred in this case.

The Arbiter requests to receive the actual messages which were exchanged between the parties in October and November which should help a lot in understanding what actually happened."[10]

When presenting their evidence on 04 June 2025, Foris stated:

a. Crypto.com only had one contact number from the Complainant as user of their services.

b. SMS confirming OTP to link card to Apple Pay as well as confirmation of such uploading to Apple Pay were sent by SMS to the Complainant's registered mobile device.

c. Both SMS were sent to Complainant on 28 October 2024.

[10] P. 34 - 37

d. For each of the disputed 8 transactions, Crypto.com sent an email and a push notification to Complainant on the Crypto.com App.

e. All disputed 8 transactions were affected through Apple Pay, which must mean that Complainant *"must have given authority for the link, whether by himself or through a third party, as this (*OTP*) was only sent to his registered mobile device".*[11]

f. Matter was elevated to VISA who also rejected the chargeback request.

g. Crypto.com would only send OTP SMS to link a card with Apple Pay to the customer registered device and at the request of such client, not at their own initiative.

No cross-examination was forthcoming on the part of the Complainant.

The Arbiter requested Foris to present documentary evidence showing SMS sent to Complainant on his registered mobile device in connection with the linking of his VISA card to Apple Pay. Foris submitted a log showing SMS history showing confirmation of uploading the card to Google Pay on 14 August 2024 and to Apple Pay on 28 October 2024 at UTC time 19:21:05 equivalent to CET 21:21:05.[12]

Complainant submitted evidence of SMS he received on 28 October 2024 at CET 20:20 giving OTP for adding his card to Apple Pay.[13]

It is evident that between 20:20 and 21:21:05 of 28 October 2024, the VISA card was uploaded on to Apple Pay.

Final submissions

In his final submissions, Complainant submitted new evidence related to GDPR issues on the use by Foris of an SMS service provider for which he never gave consent and that he reported as unreliable. In accordance with normal procedures, no new evidence is accepted at the stage of final submissions, and

[11] P. 39
[12] P. 43
[13] P. 46

this apart from the fact that the Arbiter is not the right Authority for reporting GDPR issues.

In their final submissions, Foris reported they are unable to provide evidence, as requested by the Arbiter, of Complainant's request to link his VISA with Apple Pay as they hold no such records.[14]

Foris reiterated that the disputed transactions were authorised by Complainant possibly through his gross negligence by providing to third parties the OTP to link his card to Apple Pay.

Unsolicited further submissions were made by Complainant following the Service Provider's final submissions, but these are not being considered in this process.

Analysis and considerations

The crucial issue of this Complaint is whether:

- the disputed transactions were unauthorised by the Complainant and should therefore be fully refunded in terms of Article 73 of PSD 2

  or

- these transactions were authorised by the Complainant directly or by a fraudulent third party through the Complainant's gross negligence by disclosing his access credentials permitting a such third party to link his card to Apple Pay and then execute the transactions with what, from the Service Provider's view, appeared as authorised transactions.

There is no dispute that on 28 October 2024, Complainant attempted to make an online purchase from what he describes as a fraudulent website that he clicked upon following a Google search.

Complainant admitted that in the process of trying to make such purchase, he input on the website his VISA card number, its expiry date and the three digit CVC but he did not input the code to link his Apple Pay provided by Foris.

[14] P. 56

However, in his complaint letter to Service Provider[15] he states, *"without my knowledge, this site used the OTP code received by SMS to add my card to Apple Pay".*

It is inexplicable how a merchant could use an OTP sent on the personal mobile of Complainant without the latter disclosing it. Furthermore, the Complainant was very inconsistent on whether he had received SMS from Foris regarding linking his card on to Apple Pay. At one stage, he says he does not read SMSes from Crypto.com.[16] In other parts of his evidence, he acknowledges he had the OTP code (therefore, he had read the SMS) but did not input it on the fraudulent website because it turned blank before he could input it.[17]

The Arbiter does not understand why a person should input such OTP on a Merchant website to upload his card on Apple Pay. Such OTP is not part of the online purchase through the website and should have been used only by the Complainant to upload his VISA on Apple Pay. If he did not request such upload, and if he did not possess an Apple phone, he should have reported this matter immediately to the Service Provider. Instead, he explains that he tried to input it on the merchant's website but failed.

The strong balance of probability is that in the process of trying to execute the online purchase on 28 October 2024, the Complainant not only disclosed his card details as he admitted, but he (inadvertently?) also disclosed the OTP that enabled linking his card to Apple Pay. Which channel was used for such disclosure is not clear.

In his decision, the Arbiter will have to consider whether this would amount to gross negligence which would be a justifiable reason for the Service Provider to deny refund.

Preamble 72 of the PSD 2 states:

> *"In order to assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should*

[15] P. 8
[16] P. 36
[17] P. 35

> *generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties. Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer should be considered to be null and void. Moreover, in specific situations and in particular where the payment instrument is not present at the point of sale, such as in the case of online payments, it is appropriate that the payment service provider be required to provide evidence of alleged negligence since the payer's means to do so are very limited in such cases."*

In this particular case, having established the high probability (in the absence of any other logical explanation) that the Complainant actually divulged his card details and the OTP linking it to Apple Pay to the fraudulent merchant, the situation is equivalent to the example of what amounts to gross negligence in the above-quoted preamble:

> *"for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties."*

For this reason, the Arbiter sees no case for upholding the first complaint stating:

Article 73 of PSD 2 (EU Payments Services Directive 2015/2366)[18] mandates a swift refund of unauthorised transactions in the absence of strong authentication.

The Arbiter also considers the second complaint that the fraud was facilitated by the Service Provider not operating a Strong Customer Authentication (SCA) as contemplated in the PSD2.

[18] Article 73 is reproduced in an annex to this decision.

SCA is an authentication process that validates the identity of the payment services user (PSU) or of the payment service. More specifically, the SCA indicates whether the use of the payment instrument is authorised. SCA is based on the use of at least two elements of the following three categories:

- **Knowledge**, being something only the PSU knows (such as PIN or password);
- **Possession**, being something only the PSU possesses (such as a credit card or a registered device); and
- **Inherence**, being something which the PSU is (such as the use of fingerprint or voice recognition).

In this case, the SCA was satisfied by the Knowledge of the OTP and the Possession of the mobile device on which the OTP was communicated. At no stage did Complainant indicate that he had lost possession of his device, so having the Knowledge and Possession on same device does not prejudice either.

The Arbiter accordingly concludes that the payments in question were properly authenticated and, moreover, they were, from the point of view of the Service Provider, properly authorised through the gross negligence of the Complainant.

Regarding the third complaint that Foris have inadequate fraud detection systems which would have flagged the payments as suspicious, the Arbiter again finds no evidence to support this claim. The payments were individually, and to a lesser extent even collectively, for relatively small amounts which would not normally trigger suspicions of fraud. Furthermore, they happened in very quick succession requiring a non-compulsory real-time transaction monitoring in order to trigger any concern.

Payment Service Providers (PSPs) are obliged to have effective monitoring systems of payments to protect their PSUs from payments frauds. Commission Delegated regulation (EU) 2018/389 of 27 November 2017 establishes regulatory technical standards for strong customer authentication and common and secure open standards of communication supplementing Directive (EU) 2015/2366.

It states in article 2(1) that:

“Payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorised and fraudulent payment transactions … those mechanisms shall be based on the analyses of payment transactions taking into account elements which are typical of the payment service in the circumstances of a normal use of the personalised security credentials.”

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

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

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

In the circumstances, the Arbiter sees no evidence of any failure by Foris to detect the fraud payments in real time.

As to the last complaint that there was insufficient communication on Foris’s part to inform about the registration of his card on Apple Pay, the Arbiter finds more fault on the part of the Complainant who admits he does not read Foris’s SMS notifications.

However, the Arbiter expresses concern that Foris could not provide evidence of the request they received to link the card to Apple Pay although they explain that

this could have only been triggered by the card user and the OTP, and confirmation of uploading on to Apple Pay were both sent to card user by SMS on the mobile device registered in their records.

Decision

For reasons explained above, the Arbiter is dismissing this Complaint and orders the parties to carry their own costs of these proceedings.

_____

Alfred Mifsud
Arbiter for Financial Services

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.

Annexe

Article 73 of PSD 2

Payment service provider's liability for unauthorised payment transactions

1. Member States shall ensure that, without prejudice to Article 71, in the case of an unauthorised payment transaction, the payer's payment service provider refunds the payer the amount of the unauthorised payment transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the transaction, except where the payer's payment service provider has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing. Where applicable, the payer's payment service provider shall restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. This shall also ensure that the credit value date for the payer's payment account shall be no later than the date the amount had been debited.

2. Where the payment transaction is initiated through a payment initiation service provider, the account servicing payment service provider shall refund immediately, and in any event no later than by the end of the following business day the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place.

   If the payment initiation service provider is liable for the unauthorised payment transaction, it shall immediately compensate the account servicing payment service provider at its request for the losses incurred or sums paid as a result of the refund to the payer, including the amount of the unauthorised payment transaction. In accordance with Article 72(1), the burden shall be on the payment initiation service provider to prove that, within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical

breakdown or other deficiency linked to the payment service of which it is in charge.

3. Further financial compensation may be determined in accordance with the law applicable to the contract concluded between the payer and the payment service provider or the contract concluded between the payer and the payment initiation service provider if applicable.