Regulating Digital Asset Platforms Proposals Paper

Submission to the Australian Government - Treasury

December 2023

afca
Australian Financial Complaints Authority

Contents

Introduction

The Australian Financial Complaints Authority (**AFCA**) is the independent external dispute resolution (**EDR**) scheme for the financial services sector. For over 25 years, AFCA and its predecessor schemes have provided a cost-free, fair and independent, forum for Australian consumers and small business to have their financial complaints resolved. AFCA also works with financial firm members to improve their processes and understanding of issues driving complaints to raise industry standards of service.

In addition to resolving individual complaints, AFCA has responsibilities[1] to identify, resolve and report on systemic issues and to notify the Australian Securities and Investments Commission (ASIC), and other regulators, of serious contraventions of the law.

Since its establishment on 1 November 2018, AFCA has handled over 400,000 complaints and delivered over $1.2 billion in compensation and refunds to Australian consumers and small businesses. Its systemic issues work has resulted in 4.8 million people receiving more than $340 million in compensation. AFCA therefore plays a key role in restoring trust in the financial services sector and is committed to delivering fair, efficient and timely dispute resolution services, to meet the needs of the diverse communities we serve.

AFCA welcomes the opportunity to provide a submission[2] in response to Treasury's Regulating Digital Asset Platforms Proposals Paper (the Proposals Paper). We understand from the Proposals Paper that the Government is looking to introduce a regulatory framework for entities providing access to digital assets and holding them for Australians and Australian businesses. We note in particular that the Treasury Factsheet accompanying the Proposals Paper states that:

> *Extending these types of obligations to digital asset platforms will decrease the risk of crypto exchange collapses, protecting the assets of Australians who use these platforms ... It will increase scrutiny on exchanges to ensure their customers are well informed, and reduce the risks of consumers being impacted by scams involving crypto.*

Our submission focuses on these objectives.

[1] Refer to Part C, Reporting Requirements, of ASIC Regulatory Guide 267: Oversight of the Australian Financial Complaints Authority.
[2] This submission has been prepared by the staff of AFCA and does not necessarily represent the views of individual directors of AFCA.

Executive Summary

AFCA understands that in line with the Proposals Paper, Digital asset platforms (DAPs) will be required to hold an Australian Financial Services (AFS) license[3] and comply with the General Obligations under s912A of the *Corporations Act* (the Act). These obligations include having appropriate dispute resolution and compensation processes in place for retail clients, consistent with Australian Securities and Investment Commission's (ASIC) Regulatory Guide 271 Internal Dispute Resolution (IDR) (RG271).

The Proposals Paper does not explicitly refer to EDR arrangements and consumers rights if they are not satisfied with a DAP's response to their IDR complaint. However, as AFCA membership forms part of the licensing requirements in the Act we therefore understand our service will form an important part of the consumer protection framework for consumers who use DAPs.

There are currently eight DAPs, relevant to this inquiry, who are members of AFCA. These members are identified in Appendix 1. We understand this number may significantly increase as a result of the proposed licensing reforms.

Some DAPs that facilitate the trade of cryptocurrency have become voluntary members of AFCA, as they currently do not require an AFS licence to operate. DAPs that provide exchange services for other financial products and services (i.e., CFDs, ETFs etc.) already hold an AFS licence for those regulated activities and are required to become AFCA members.

The common thread to many DAP complaints AFCA receives, especially complaints that proceed to an Ombudsman determination, is the prevalence of scams. As there are currently no obligations on DAPs to meet accepted standards of scam mitigation measures, and given their contracts tend to place the risk of using DAPs on to consumers, there are few avenues for redress available to consumers who lose money as a result of scams, particularly involving cryptocurrency transfers to third parties. As a result, most determinations issued by AFCA in these cases are in favour of the financial firm member.

Based on our experience in dealing with complaints about DAPs, and having regard to the proposed objectives of these reforms, AFCA supports the proposal to require DAPs to obtain an AFS licence and calls for:

1. Clear and fit-for-purpose regulatory rules that reflect the unique challenges presented by digital asset transactions and measures to reduce the frequency and financial impact of scams (especially relating to cryptocurrency).

[3] Subject to an exemption where the total value of platform entitlements held by any one client of the platform provider does not exceed $1,500 at any one time; and the total amount of assets held by the platform provider does not exceed $5 million at any time.

2. Clear and fair standards for standard form contracts that are informed by some of the issues that AFCA has seen arise in complaints. It will also be important to ensure that standard form facility contracts and platform terms of use do no override or interfere with proposed obligations being built into the regulatory framework, including avenues for consumers to seek redress.

3. Appropriate financial requirement obligations on platform providers that support their ability to comply with any AFCA determinations made against them.

4. Clarity about what is and isn't regulated to minimise the risk of regulatory arbitrage and consumer confusion and exclusion from the dispute resolution framework.

AFCA's complaints experience

Platform Provider Complaints

AFCA has considered approximately 1,140[4] transactional complaints about DAPs[5], with 46 complaints being the subject of Ombudsman determinations. As mentioned, the majority of determinations issued by AFCA in these cases involve complainants who were the subject of a scam by an unrelated party after using a provider's platform to transfer payment, believing they were investing in cryptocurrency.

These complaints have included cases involving six figure losses, vulnerable consumers and where funds were a large part of a complainant's retirement savings.

When considering complaints involving DAPs, AFCA has regard to the contract entered into by the client with the DAP and the relevant terms in relation to the issue the subject of the complaint. The contract and related platform terms of use form the basis for AFCA to determine if a DAP has met its obligations to clients, particularly for complaints relating to voluntary members.

The effect of this is that while consumers in principle have access to EDR, in practice there are few realistic avenues for redress available to them where losses are caused by scams or other fraudulent conduct. This should be considered when designing the proposed regulatory framework.

Scams and industry mitigation measures

AFCA is of the view that there is a reasonable community expectation that organisations should be doing all in their capacity to disrupt scam activity and ensure consumers who use their service can have a high level of trust that they are protected. This extends to an expectation that if scam activity is facilitated through the

[4] Total complaints include complaints considered by predecessor scheme – Financial Ombudsman Service. This total also includes complaints (approx. 465) received against Forex Financial Services Pty Ltd (FFS). FFS was taken over by IFS Markets which was ultimately taken over by FTX Australia Pty Ltd.
[5] See appendix 1 for the list of Platform Providers referenced in AFCA's submission.

services offered by a financial firm, then that firm will put measures in place to reduce the likely recurrence and where possible take steps to retrieve these funds.

In relation to DAPs, we have seen that consumers are often unaware that some of the scam mitigation measures and initiatives in place in other sectors, are not present with DAPs. While AFCA acknowledges the challenges the industry faces in order to combat scam activity, especially relating to crypto, implementing accepted standards and procedures for scam mitigation could assist to rebalance the disproportionate level of liability currently borne by consumers. This is discussed further below.

In our experience with crypto-related cases, complainants have also faced the following issues in order to prove that the DAP was or should have been on notice about a scam:

- The DAP's due diligence calls not being recorded - and therefore the call and its content disputed by the client. (AFCA notes and supports the Government's intention to have Know Your Client (KYC) obligations embedded in the framework, along with other standards that look to reduce the risk, and respond to, instances of fraud and other harms).
- Being "coached" by the scammer to pass a DAP's due diligence calls.
- An inconsistent patchwork of information sharing and mitigation measures.

Some measures that may assist DAPs to proactively identify potential scams and red flags before an issue occurs could include:

- proper identity checks on recorded lines (we have seen a recent example of an allegation of the scammer imitating the complainant on the due diligence call).
- industry wide 2 factor authentication for set up of accounts and ongoing access, to ensure any transactions are authorised by the client.

AFCA Determinations

Following are two examples of Ombudsman determinations issued in complaints against DAPs. These examples are typical of the complaint outcomes where a complainant was subject to a scam, facilitated through a platform. In these cases, AFCA found that the member firms had complied with the terms and conditions of use.

Scams and contract terms

The complainant was the victim of a scam by an organisation after using the financial firm's platform to transfer payment to the scammer, believing he was investing in cryptocurrency mining.

The complainant said the financial firm authorised and executed his transactions and this caused him to lose money. In attempting to secure the return of his funds, the complainant provided two further payments to the scammer. Soon after, the scammer stopped communicating and the funds were no longer available.

The complainant said the financial firm failed to alert him to a potential scam and proceeded to authorise and execute the transactions. The financial firm said there are warnings against transfers from its platform to unknown recipients and adequate security recommendations were provided to the complainant.

The financial firm also said that due to the anonymous nature of cryptocurrencies, it is unable to identify recipients that are not using its platform and it is unable to identify the owners of cryptocurrency addresses. It states there are warnings against transfers from its platform to unknown recipients and adequate security recommendations were provided to the complainant.

The ombudsman concluded that the transfers of the complainant's funds were made to an organisation unrelated to the financial firm. The terms of use of the platform were clear that it assumed no responsibility when cryptocurrency funds are transferred from its platform to another site. Despite the complainant's expectations, the terms of use did not give any indication that the financial firm would undertake due diligence to test the legitimacy of third parties. Based on these considerations, the ombudsman found that the financial firm was not liable for the actions of that organisation.

Reliance on onboarding call

This complaint relates to a loss sustained during cryptocurrency trading in which the complainant lost Coin as the result of the fraudulent conduct of an unrelated third party. The complainant said the financial firm should have protected him from the fraudulent activity of the third party, as they were known to be a scammer. The complainant said the financial firm should have identified this and flagged or prevented subsequent transfers from his account to them.

The complainant lost $49,891.53 which he said was much of his life savings. He said he was over 65 years of age and was unemployed. The complainant submitted that the financial firm had responsibility to its customer, and it was its negligence that caused the loss. He said the financial firm was responsible for keeping his money secure and there should have been processes in place that protect the customer's monies.

The financial firm said due to the anonymous nature of cryptocurrencies, it cannot identify the recipients of Coins transferred from its accounts. The financial firm relied on the terms of use and an onboarding telephone call in contending the

complainant was aware of its process and the risks involved in customers transferring Coins to other entities.

The complainant said he never received an onboarding call. The financial firm, in response, provided a telephone record showing a call placed to the complainant's mobile telephone number. The corresponding account note showed that during this call the complainant was warned specifically about investment scams and that transactions cannot be reversed.

The ombudsman was satisfied the onboarding call was made and that during this call the complainant was notified as to the effect of the relevant terms of use. The ombudsman concluded that the complainant acted contrary to the security warnings given by the financial firm and made the decision to invest through the unknown third party.

Given the terms of use, the ombudsman was satisfied the financial firm was not responsible for the transfer of Coins to a third party in the event of a scam and the terms of use absolved it from liability in such circumstances.

Proposed Mandatory Industry Codes - scams

The Government has issued a consultation paper which seeks feedback on its intention to introduce mandatory industry codes to combat scam activity and increase obligations on specific sectors to undertake anti-scam preventative measures[6]. The primary objective of the codes will be to set clear roles and responsibilities for the Government, regulators, and the private sector in combatting scams. This includes ensuring key sectors in the scams ecosystem have appropriate measures in place to prevent, detect, disrupt, and respond to scams, including sharing scam intelligence across and between sectors.

The proposal paper also says that where a business fails to meet its obligations under the framework, IDR and/or EDR mechanisms would ensure consumers have access to appropriate redress, and regulators would be given new enforcement and penalty powers.

The codes and standards being contemplated will initially cover the following sectors:

- Banks
- Telecommunication Providers
- Digital Communication Platforms

AFCA notes that the implementation of the Scams Code Framework is subject to future Government decisions, and legislative design and development. As DAPs are often a gateway for crypto scams, this sector should be required to have the same measures in place as contemplated by the proposal paper to prevent, detect, disrupt,

[6] Scams – mandatory industry codes | Treasury.gov.au

and respond to scams. A sector specific code for this industry should also be considered and could assist in minimising consumer harm.

Consumer understanding

Another theme present in many DAP complaints is consumers' overall understanding of crypto/digital assets, including a general lack of understanding of their associated risks. We also seen cases where consumers were unaware:

- Whether the DAP used a third-party custodian, and whether they understood the significance of this.
- whether they have actual ownership of the underlying asset or if they are dealing with a derivative; and

To promote confidence in the use of DAPs, it is essential that consumers understand the nature and the risks of the service they are using and whether they are investing in crypto or derivatives.

Standard form facility contracts

While our complaint experience shows that DAPs generally have some measures in place to warn clients about the risks associated with the use of their platforms, these measures have not sufficiently prevented or disrupted significant consumer loses. In AFCA's experience, consumers are also often unaware of:

- how broad indemnities and contract terms:
  - interact with Platform Providers obligations, and
  - limit Platform Providers liabilities
- how contract terms will be applied in practice
- what conduct falls within or outside the contract terms
- any measures Platform Providers are required to and/or have in place to protect consumers from financial harm as a result of using their platform.

In AFCA's view, these contracts are weighted too heavily towards protecting DAPs by transferring the risk, and therefore liability, for many issues that occur on or facilitated through a DAP to consumers. AFCA supports the Proposals Paper focus on DAPs issuing standard form facility contracts that include:

- a set of minimum standards
- non-discretionary rules and arrangements, and
- a set of transparent and non-discriminatory criteria governing platform access.

As mentioned, these contracts should have a focus on supporting consumer understanding of potential risks associated with using the relevant platform, and any limits on DAP liabilities, and be fair to both parties.

Financial requirements

Platform Providers do not currently form part of the Compensation Scheme of Last Resort (CSLR) framework. It is important therefore that they are required to meet standard AFS license obligations, including:

- Financial requirements (for example, solvency and cash) in line with Regulatory Guide 166 *Licensing: Financial requirements* (RG166), and
- Compensation and insurance arrangements (including Professional Indemnity insurance) in line with Regulatory Guide 126 *Compensation and insurance arrangements for AFS licensees* (RG 126).

This will assist in mitigating the potential for Platform Providers failing to have capacity to meet their license obligations, including complying with AFCA determinations that may award financial compensation to complainants.

Case Study – FTX Australia Pty Ltd

Uncompensated losses and Licence acquisition

Uncompensated losses

FTX Australia Pty Ltd became a member of AFCA after acquiring AFS licensee IFS Markets in 2021. IFS Markets previously obtained its AFS license after acquiring Forex Financial Services Pty Ltd (FFS). FFS was a member of AFCA (and its predecessor scheme - FOS) since 2009. In November 2022, ASIC suspended the Australian financial services licence of FTX Australia after it was placed into voluntary administration.

AFCA received a batch of complaints against FTX Australia at that time (approx. 66). These complaints included individual claimed losses of over $300,000. As FTX was unable to pay its debts, which included consumer claims for compensation, the majority of complaints were put on hold while AFCA waited for the CSLR to be established and its scope finalised.

On 22 June 2023, the Parliament of Australia passed legislation to establish the CSLR and limited its scope to complaints about financial firms that:

- provide financial product advice to retail clients
- deal in securities for retail clients, and
- engage in regulated credit activities.

Because FTX complaints did not relate to a financial product or service captured by the CSLR, AFCA cannot resolve these complaints efficiently, effectively, or fairly, as required under Rule A.2 and s1051(4)(b) of the Corporations Act. AFCA has therefore exercised its discretion under the AFCA Rules to not consider these complaints and has communicated this information to the majority of FTX complainants.

Licence acquisition

ASIC cancelled the licence held by FTX Australia Pty Ltd (FTX Australia), effective from 14 July 2023.

The Parliamentary joint Committee on the Corporations and Financial Services issued a report in July 2023 in response to its *Statutory inquiry into ASIC, the Takeovers Panel, and the corporations legislation: ASIC licence transfers.* The Committee expressed concern about the circumstances in which FTX obtained its AFS license before it collapsed. As part of its final report[7], the Committee recommended the following:

'The committee recommends that ASIC examine the transfer or change in control of all high-risk licences including market licences, benchmark operator licences, clearing and settlement licences, and any financial service or credit licence transfers or changes in control that have high-risk features due to the scale or complexity of the service to be provided under the licence.'

Given the potential for organisations to enter into the DAP space by acquiring an existing AFS licence, this recommendation appears to offer a sensible safeguard. If adopted, AFCA may be able to contribute to any examination by providing complaint data insights about the existing AFS licensee.

The proposed framework

For AFCA to be able to effectively deal with complaints under the proposed framework it is essential that there is also clarity about:

- what tokens represent a financial and non-financial product
- DAP obligations in all circumstances (including when the token holds a financial and non-financial product), and
- the potential consequences for failing to meet the relevant obligations.

We highlight the following areas that have the potential to cause uncertainty about how or if AFCA may consider certain complaints against DAPs:

Topic	Comment
Interaction between the existing AFS license framework and new financialised function regime.	The reforms aim to accommodate a diverse range of entitlements being recorded in token-based systems (i.e. 'tokenised') and look to address the financialisation of non-financial entitlements.

[7] Statutory inquiry into ASIC, the Takeovers Panel, and the corporations legislation: ASIC licence transfers – Parliament of Australia (aph.gov.au)

Topic	Comment
	If there is no existing law or framework for the specific activity of Platform Providers, there will be new measures put around it. In some cases, the proposed framework may be 'engaged to supplement the existing regulatory framework'. It will be important to ensure that Platform Providers are aware of their obligations under the existing AFS license framework and: 1. how this interacts with the financialised function regime for non-financial product 2. what tokens are defined as a financial and non-financial product, and 3. if the proposed framework is engaged to supplement the existing legal/regulatory framework, that there is clear guidance on how these interact and in what circumstances.
Potential for regulatory grey zones	The intention is to regulate digital asset platforms rather than the various digital assets. A stress point may be to ensure new technologies do not get ahead of regulation to create grey zones (regardless of the tech. agnostic intention of the proposals).
EDR considerations	AFCA is likely to receive complaints against a Platform Provider that holds entitlements to financial and non-financial product assets. AFCA would look to the regulations to determine the obligations on Platform Providers in these scenarios, and what avenues of redress are available to consumers if the Platform Provider fails to meet their obligations under the proposed framework. If the regulations are not clear, it may fall to AFCA and potentially the courts to determine appropriate financial remedies in the circumstances.
Platforms exempt from regulation	The exemption provision may see consumers with smaller tokens excluded from IDR/EDR avenues for redress as their platform provider is exempt from a requirement to hold an AFS license. This design leaves out smaller platforms (not exceeding $5M platform total assets and not holding any individual entitlement of $1,500 at any one time). While it is understood the focus is on regulating where there is potential avenue for significant loss, the exemption will likely see entities create platforms to elude regulation and capture this market (which may target less sophisticated and financially buffered participants).

Topic	Comment
	While individual losses may not be significant at one time, they could become so if a consumer continues to add tokens after past losses and may be significant commensurate to their financial situation. The cumulative gain a Platform Provider might obtain if they capture the small trade market may be significant. Any conduct issues stemming from these exempt platforms, including of a systemic nature, will unlikely be readily identifiable without regulatory oversight and opportunity for IDR/EDR.

Appendix 1.

1.1 Crypto platform members and complaint statistics

Below is a list of current or recently exited voluntary AFCA members offering cryptocurrency platforms.

Member name	Status	Joined AFCA/FOS[8]	Total complaints	Closed at Rules	Closed Reg & Ref	Closed at Decision
BTC Markets	Ceased (Nov 23)	Feb-17	98	5	48	9
Casey Block Services	Effective	Aug-17	381	17	120	35
Cryptospend Pty LTd	Effective	May-23	3	0	2	0
Foris Dax Au Pty Ltd	Effective	Apr-21	36	3	10	3
Foris GFS Australia Pty Ltd	Effective	Dec-20	23	2	16	0
FTX Australia Pty Ltd (in admin – still member)[9]	Effective	Aug-09	537	467	1	0
Independent Reserve Pty Ltd	Ceased (March 21)	Jul-17	22	3	9	2
Oztures Trading Pty Ltd	Effective	Nov-11	40	7	3	0

[8] Financial Ombudsman Service (FOS) – Predecessor scheme to AFCA.
[9] Total complaints include complaints considered by predecessor scheme – Financial Ombudsman Service. This total also includes complaints (approx. 465) received against Forex Financial Services Pty Ltd (FFS). FFS was taken over by IFS Markets which was ultimately taken over by FTX Australia Pty Ltd (FTX). Complaints against FTX were limited to complaints received when the financial firm entered Administration.