swyftx

Scams – Mandatory Industry Codes

Response to Treasury Consultation Paper

swyftx

29 January 2024

Scams Taskforce
Market Conduct and Digital Division
The Treasury
Langton Crescent
Parkes ACT 2600

By email: scamspolicy@treasury.gov.au

Dear Treasury

Swyftx's submission to the Scams – Mandatory Industry Codes Consultation Paper

Introduction

Thank you for the opportunity to provide this submission in response to the Scams – Mandatory Industry Codes Consultation Paper (**Paper**). Our submission continues a long history of engagement with Treasury and the Government for over two years regarding regulatory matters relevant to the crypto sector, and we do not take for granted Treasury's willingness to continually engage with our industry and hear our respective voices.[1]

Over the past two years, much of the regulatory discourse surrounding the crypto sector has focused on the failures of centralised actors and the regulatory obligations that ought to be applied to protect against future investor harm. In Australia, this is currently the subject of Treasury's recent Regulating Digital Asset Platforms Proposal Paper. However, during the same period, scam activity rose dramatically in Australia and around the globe, moving the Australian Government to take swift action to make combatting scams a priority.[2]

Just as we support the proposed Digital Asset Facility licensing framework to protect Australian investors, we are equally supportive of robust industry requirements to protect Australians from scams. Accordingly, we think the crypto sector should be subject to a mandatory code under the proposed framework outlined in the Paper, and we agree with Treasury's "whole-of-ecosystem" approach to addressing scams.

Swyftx and financial crime

There are features of blockchain-based systems that can be attractive to scammers (eg, immutable ledgers with transaction speed and finality). Because of this, we recognised early the need for an effective fraud program. This was to complement (and was in addition to) the work we had been doing since inception to comply with our regulatory obligations as a reporting entity under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**).

---

[1] Senate Select Committee on Australia as a Technology and Financial Centre (Submission 21), Treasury's Crypto Asset Secondary Service Providers: Licensing and Custody Requirements Consultation Paper (Swyftx Submission), Treasury's Token Mapping Consultation Paper (Swyftx Submission), the Attorney-General's Department's Modernising Australia's Anti-Money Laundering and Counter-Terrorism Financing Regime Consultation Paper (submitted but not yet made public), and Treasury's Regulating Digital Asset Platforms Proposal Paper (submitted but not yet made public).

[2] Assistant Treasurer and Minister for Financial Services' announcement of the National Anti-Scams Centre (15 May 2023) and ACCC's Targeting scams: report of the ACCC on scams activity 2022 (17 April 2023).

We have an established Financial Crime team that is devoted to combatting fraudulent activity detected on our platform, including where we suspect customers could be the victim of scams.

Today, we are a recognised leader in the financial crime community for the work we do on scams, including our involvement in the following groups and forums:

- Associate member of Interbank;
- Member of the Telecommunication Fraud Forum;
- Member of the Economic Crime Forum;
- Member of the Australian Financial Crimes Exchange (**AFCX**) Fraud Reporting Exchange (FRX);
- Member of the Financial Services Information Sharing and Analysis Center (FS-ISAC); and
- Participation in Fintel Alliance, and the National Anti-Scam Centre (NASC).

Mandatory Scam Code for Crypto

While we appreciate the crypto sector may be a 'future' rather than 'initial' sector to be covered under the framework, we are confident that we (and we suspect, many other crypto exchange operators) would be able to comply with many of the proposed obligations outlined in the Paper. We believe that the proposed code should apply to the crypto sector as soon as possible. If Treasury aligns with this approach, we suggest that the proposed code apply to all digital currency exchange providers, as under the AML/CTF Act.

Swyftx Scam Practices

Given the importance we place on customer safety, we already have practices in place that would comply with most of the proposed ecosystem-wide obligations in the CCA. Subject to clarification on the proposed verification of information (as noted below), the only change we would likely need to implement from the proposed obligations is an anti-scam strategy to complement our existing Fraud Program. At present, our Fraud Program covers fraud and scam prevention, detection, disruption and response, but we would welcome the opportunity to further bolster this to comply with the anti-scam strategy proposals.

Our interpretation of the obligation to "provide … consumers or users with tools to verify information in real time" is that a customer must be able to verify the validity of communications through a secure method. If this interpretation aligns with the drafting intention, we would welcome greater clarification to the current wording (and note that, in any event, we would be compliant).

With respect to the proposed bank-specific obligations (should they apply to a business such as Swyftx), we have already implemented, among others, the following practices:

- identification of higher risk consumers and activity, as well as taking appropriate steps to warn, block or suspend transactions, and blocking or disabling scammer accounts; and
- methods and processes to identify and share information with other banks that an account or transaction is likely to be or is a scam, and to act quickly on information received by blocking or disabling the scammer account. As noted in the Paper, as a member of the AFCX, this is presently one of the avenues where we achieve this information sharing. AFCX are also chairing a Digital Currency Exchange Blacklist Wallet Sharing pilot program, with Swyftx and two other exchanges to further the crypto industry's ability to allow this sharing of information to prevent more scams.

Application to the Crypto Sector

Whilst we are a proponent for proposed framework, there is a key nuance that needs to be considered in applying the obligations to the crypto sector, which is the irreversible nature of most crypto transfers. This characteristic would, in most cases, make a tracing and recovery obligation very difficult to comply with. It is for this reason that we have invested so heavily in our Financial Crime resources and procedures, including our sophisticated, internally developed in-house transaction monitoring program.

Additionally, we believe that the specific risks associated with the crypto sector are greatly mitigated by educating our customers about detecting and avoiding scams. To achieve this, we have developed the following educational resources:

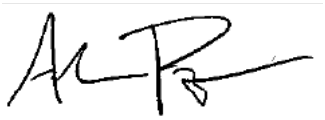
- Swyftx Website – Security Learn (link): A dedicated section of our educational platform offering users insights into safeguarding their accounts and transactions and how to spot scams. There are currently 14 articles focused on these topics;
- Scams Learn and Earn Module (link): Our 'Scams Learn and Earn' module serves as an interactive educational tool, enabling users to enhance their understanding of potential scams in the investment landscape and how to safeguard their account. As part of an innovative pilot to see if we could incentivise customers to protect themselves, Swyftx, in collaboration with TRM Labs, offered the first 2,000 customers $10 in Bitcoin who completed the module and enabled two-factor authentication (2FA);
- Ongoing Scam Awareness Marketing Campaign: We regularly run scam awareness marketing campaigns, leveraging various channels, including social media posts and email campaigns; and
- Dedicated Customer Support and Financial Crime Staff: Our customer support and financial crime staff are equipped and trained to provide personalised scam awareness and education, offering users direct assistance in understanding and mitigating potential risks.

In closing, we support the proposed framework and welcome the opportunity to afford greater protection to our customers against fraud and scams. We urge Treasury to consider the nuances within the crypto sector and would welcome the opportunity to discuss any aspect of our submission with you in greater detail.

We appreciate the opportunity to provide this submission. If you have any questions, please do not hesitate to contact me at Adam.Percy@swyftx.com.au, or Gabby Lewis, Financial Crime Manager, at Gabby.Lewis@swyftx.com.au.

We look forward to our continued engagement with both Treasury and the Government on these critical issues.

Yours faithfully



Adam Percy
General Counsel & Company Secretary
Chief Risk & Compliance Officer
Swyftx Pty Ltd