ARBITER FOR FINANCIAL SERVICES

Technical NOTE

Guidance on considerations that the Arbiter will adopt in determining complaints related to 'pig butchering' type of scams

Contents

Revisions Log

Version	Date Issued	Details
1.00	11 February 2025	Issuance of Technical Note

Acronyms & Abbreviations

AML/FT:	Anti-Money Laundering and Financing of Terrorism
APP:	Authorised Push Payment
B2B:	Business-to-Business
ESMA:	European Securities and Markets Authority
FIAU:	Financial Intelligence Analysis Unit
IBAN:	International Bank Account Number
KYC:	Know Your Customer
OAFS:	Office of the Arbiter for Financial Services
PSD2:	Payment Services Directive 2
PSP:	Payment Service Provider
PSU:	Payment Service User
USDT:	Tether (a type of cryptocurrency)
VASP:	Virtual Financial Assets Service Provider
VFA:	Virtual Financial Assets

A. Background

Following the model issued by the Arbiter in December 2023 regarding the allocation of responsibility between a Payment Service Provider ('PSP') and a Payment Service User ('PSU') in case of payment fraud scams, the Arbiter now considers it timely to similarly issue general guidance about the considerations relevant to complaints involving other emerging sophisticated scams, like those commonly known as 'Pig Butchering' scams.[1]

Scammers are continually evolving their schemes to defraud innocent and vulnerable financial consumers of their hard-earned savings. 'Pig Butchering' is one of the evolving and serious fraudulent schemes that have escalated rapidly in recent years. It often causes grave consequences to the victim beyond the direct impact of significant financial loss. Besides the devastating financial consequences, it can have grave emotional consequences, including one's self-confidence and self-respect, possibly leading to tragic conclusions.

Having seen a rise in complaints involving such scams, the Arbiter is issuing this Technical Note to increase awareness and outline the considerations that will shape the Arbiter's decisions. The aim is to ensure fairness, consistency, transparency and objectivity to the complaint's process for all parties involved. Service Providers are hence encouraged to review and adopt this Technical Note.

The considerations outlined in this Technical Note are for guidance purposes only. The merits of a complaint will continue to be assessed and determined on a case-by-case basis with the particular circumstances of each case considered accordingly.

If the specific circumstances so necessitate, the Arbiter may depart from certain aspects outlined in this Technical Note or take into account and/or attribute greater importance to one or more aspects as considered appropriate. The reasons

[1] *Interpol has recently suggested substituting the term Pig Butchering with something more respectful to victims. (https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-urges-end-to-Pig-Butchering-term-cites-harm-to-online-victims). As no new term has yet gained international recognition, OAFS is temporarily continuing to use the term* ***Pig Butchering*** *to ensure that potential new victims know what we are referring to and are deterred from falling into the fraud trap. For the future, we plan to use the term 'Relationship Confidence Fraud' or similar.*

for the position taken will be duly outlined, in writing, in the Arbiter's decision with each case determined and adjudicated by reference to what, in the Arbiter's opinion, is fair, equitable and reasonable in the particular circumstances and substantive merits of the respective case.[2]

B. What is 'Pig Butchering'

***'Pig Butchering'* is a scam where the scammer may use a variety of methods, such as social engineering and psychological manipulation, to establish a relationship** (either social, romantic, or business focus), **gain the victim's confidence and trust and then, gradually and deceivingly, introduce the victim to a fraudulent investment opportunity** with the fraud typically carried out **over an extended period**, often lasting several weeks to months.[3]

In most cases, scammers **first approach victims through social media or dating apps** and may ask to take the conversation to a different platform (e.g. WhatsApp, WeChat, Telegram or other messaging app). Potential victims **might also be approached directly on messaging apps.** The **scammer would communicate regularly with the victim** with the aim **to establish and maintain a relationship.**

Once the scammer **gains the victim's trust and attention** the scammer will propose an investment opportunity, typically involving crypto-assets (but may involve other assets). The scammer will offer to train the victim to set up an account on an exchange to purchase crypto-assets, and then provide a wallet address for the victim to transfer funds in order to participate in the investment opportunity. Examples of such investment opportunities might involve:

- the offer to trade online in well-known crypto-assets (or other assets) where victims are directed to fake or cloned trading platforms that would show fictitious trading and false returns;

[2] *CAP. 555, Art. 19(3)(b)*
[3] *In the Annex to this Technical Note, there is a brief summary of typical scenarios used by scammers in pig butchering scams and other scams.*

- investment in new crypto-assets or tokens;
- high-yield investment opportunities or other investments promising high- profit levels over a short period of time.

The **fraudulent investment opportunity is designed to appear legitimate** and often **produces artificial significant gains** to keep the victim engaged and lured to deposit even more funds. **Scammers exploit psychological factors, such as the fear of missing out, to manipulate victims into starting and continuing investing.** Scammers often adopt false identity and impersonification to give the impression that they are a professional person or related to respectable licensed institutions when this is not the case.

The victim is eventually never able to withdraw funds and the fictitious profits. **In the final stages of the scam, the victim is typically asked to transfer even more funds before anything can be withdrawn** through a variety of excuses for such payment requests (e.g. service fees, taxes, etc.). A **sense of urgency** is often created at that stage **for the victim to immediately settle payment requests** with the excuse that otherwise high penalties would be incurred, their account blocked or frozen or their funds completely forfeited. These would, however, be just further **attempts to continue extracting more money from their victims.**

This type of **scam ultimately causes the victim to suffer significant financial loss,** often resulting in the **loss of a substantial portion, if not all, of their savings or even accumulation of debt.**

C. How is *'Pig Butchering'* Different from APP Scams?

It is different and probably more cruel than a phishing or smishing payment fraud or Authorised Push Payment ('APP') fraud schemes, about which the Arbiter has already issued Technical Notes on how the responsibility for the loss is to be allocated between the consumer victim and the Payment Service Provider (the PSP being the bank or financial institution making the payment).

Whereas, for example, an APP fraud is often a one-shot transaction for an amount not exceeding the daily payment limit agreed with the PSP, ***'Pig Butchering'* fraud often involves a series of transactions over a span of time** and, accordingly, generally involves much larger losses.

Given that such scam happens over a period of time (sometimes several weeks or months) and involves a series of transactions, victims who have approached the Office of the Arbiter for Financial Services ('OAFS') in recent cases filed complaints *inter alia* against banks claiming fault by their service provider for not intervening and alerting them to the scam as part of the service provider's payment transaction monitoring obligations.

D. Payment Transaction Monitoring Obligations

There are different types of licensed service providers that are particularly affected by these types of scams.

Such service providers can be divided into three different broad categories:

a. Banks/Credit Institutions licensed under the Banking Act[4]
b. Financial Institutions, including Payment Institutions, licensed under the Financial Institutions Act[5]
c. Virtual Financial Assets Service Providers licensed under the Virtual Financial Assets Act.[6]

The operating licences of the said providers impose on them different levels of obligations related to payment transaction monitoring. However, licensed service providers are subject to overall fiduciary duties to their clients in terms of the Civil Code and their licence conditions.

[4] *CAP. 371*
[5] *CAP. 376*
[6] *CAP. 590*

(i) **Banks and Credit Institutions** are considered to have a very high level of obligations for transaction monitoring to protect their clients from fraud schemes. This is also a result of the general long-term relationship between the Bank and its clients, permitting the Bank to build a reliable picture of the normal transactions that clients pass through their account. Financial Institutions and Virtual Asset Service providers may not necessarily enjoy such long-term relationships with their clients.

Banks and credit institutions are obliged to have effective monitoring systems of payments to protect their PSUs from payment fraud.

For example, 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.[7] It states in article 2(1) that:

> ***"Payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorized or fraudulent payment transactions ...***
>
> ***Those mechanisms shall be based on the analysis of payment transactions taking into account elements which are typical of the payment service user in the circumstances of a normal use of the personalised security credentials."***

Article 2(2) of the said Commission Delegated Regulation furthermore states that:

> ***"Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:***
>
> ***(a) lists of compromised or stolen authentication elements;***
>
> ***(b) the amount of each payment transaction;***
>
> ***(c) known fraud scenarios in the provision of payment services;***
>
> ***(d) signs of malware infection in any sessions of the authentication procedure;***

[7] https://eur-lex.europa.eu/legal-content/EN-MT/TXT/?from=EN&uri=CELEX%3A32018R0389

> ***(e) in case the access device or the software is provided by the payment service provider, a log of the use of the access device 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.[8] 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.

Article 68(2) of PSD2 also authorises a PSP to block payments:

> ***"If agreed in the framework contract, the payment service provider may reserve the right to block the payment instrument for objectively justified reasons relating to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument or, in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil its liability to pay."***

Anti-money laundering legislation further provides other legal basis for monitoring transactions and the freezing or blocking of accounts in case of *inter alia* suspicion of fraudulent activities.

(ii) **Financial Institutions, including Payment Institutions, licensed under the Financial Institutions Act -** The provisions referred to earlier similarly apply to payment service providers licensed under the Financial Institutions Act. Claims received from personal customers against such institutions were often based on the expectations that payments made to third-party beneficiaries indicated by the fraudsters, were made to accounts that such third parties held with the financial institution concerned. Victims, therefore, claimed recoveries from the financial institution concerned for failing to stop payments or for offering account facilities to beneficiaries involved in the fraud scheme.

[8] https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2018_4090

The merits of such claims generally depend on the pattern and size of payments involved. However, given that there might be no established history of account operations between the complainant and the PSP, it would be harder to prove fault on the PSP transaction monitoring system.

Furthermore, such claims are often challenged by the PSP on the basis that the Arbiter does not have competence to hear and adjudicate them as the complainant (victim) is not their eligible customer as defined in the Arbiter for Financial Services Act, Chapter 555 of the Laws of Malta ('the Act').

Amendments to the Act are to bring such complainants within the definition of 'eligible customer' so that the Arbiter would be able to adjudicate such claims on their particular merits. The merits could then include an **examination of the robustness of the service provider's procedures for the onboarding of B2B clients that are involved in or allow themselves to be exploited by fraud schemes.**

(iii) **Virtual Financial Assets Service Providers** – These include service providers offering services of custodial wallet and the purchase and sale of digital assets through the wallet. The services also involve the transfer of digital assets to, and from, other *digital* wallets both hosted and external.

In many of the cases received by the OAFS, the complaint related to an alleged fraudster who persuaded and actively assisted their victim to open a digital wallet account with the VFA service provider, transfer funds from their normal bank account to such wallet account, and then use the funds for the purchase of digital assets, like Bitcoin and USDT, amongst others.

These digital assets were subsequently typically then transferred by the victim, under the direction of the fraudster, to an unhosted external wallet, under the control of the fraudster where external wallets would not offer visibility of their ultimate beneficiaries. Assets received in such wallets are then transferred out by fraudsters through a complex web of transactions which make it difficult to trace their ultimate destination.

When victims ultimately realise that they have been scammed they raise a complaint against the VFA service provider claiming that the VFA provider failed to protect them from fraudsters and that they should have stopped

the transfer of their assets to the external wallet. Such complaints typically invoke the obligations of the VFA for Anti-Money Laundering and Financing of Terrorism (AML/FT) obligations or referring to provisions of the Payment Services Directive which may not necessarily apply.

In most cases adjudicated so far, the Arbiter could not uphold the victims' claim as:

1. The Virtual Financial Assets Act ('VFA Act') does not provide for similar transaction monitoring obligations that banks have under Central Bank of Malta Directive No. 1 – The Provision and Use of Payment Services (Ref. CBM 01/2018) which states that ***"This Directive is modelled on the requisites of the Directive (EU) 2015/2366".***[9]

2. AML/FT obligations are covered by Implementing Procedures issued by the Financial Intelligence Analysis Unit (FIAU) as applicable to the Virtual Financial Assets Sector.[10] However, any infringements to such Implementing Procedures fall under the prerogative and responsibility of the FIAU who may sanction the licensee as appropriate for its failure, but does not offer adjudication services in favour of the fraud victims.

E. Guidance Going Forward

i. Banks and Credit Institutions

Banks are urged to ensure that substantial upgrades have been made to their payments monitoring systems. Banks have the benefit of long-term relationships with their clients, and they **need systems which are sensitive to new patterns compared to historical trends. New patterns should be flagged, and customer needs to be alerted and advised** accordingly. **Conversations with clients are to be properly recorded** so that they may serve as evidence in the adjudication process.

Banks should be aware of common features of scams and have an **obligation to warn their client about the risk flagged**

[9] Directive-1.pdf (centralbankmalta.org)
[10] FIAU Part II (fiaumalta.org)

by abnormal deviation from their normal payments pattern and the risk that this could involve a scam. **Further enquiries and an appropriate conversation with their customer could make a difference** and prevent augmentation of a fraud scam in its nascent stage.

Banks' defence that changed pattern payments did not merit their intervention as they just involved transfer to customer's own account with a third-party bank or institution or VFA service provider are valid only up to a point.

Banks should have enough experience to raise doubts about certain crypto account operations by a retail client being untypical and raise suspicions. Untypical transfer/s should be looked upon with due suspicion even in case of me-to-me payments.

For an out-of-character transaction or once a pattern takes certain shape and amounts transferred start becoming frequent and accumulating being totally out of shape with past historical pattern of payments, Banks need to intervene to alert their customer before it gets too late.

At which point in a transaction or pattern banks should intervene to alert and have a conversation with their client depends on the circumstances of each case but doing nothing and relying on the me-to-me payments argument, will not find favour with the Arbiter.

When it comes to transaction monitoring obligations and assessment of
appropriate action by the service provider, the Arbiter shall accordingly also take into consideration the following:

- **at which point/s the bank intervened;**
- the **extent and type of intervention/s** that was taken by the bank;
- the **behaviour and actions of the complainant following any such intervention/s.**

The Arbiter will particularly take into account the above with respect to unusual or out-of-character transactions. **The considerations that would be made to determine whether a transaction is considered unusual or out-of-character include *inter alia* any one or a combination of the following in the context of previous historical transactions and the customer's profile:**

a. the a**mount and size of the transaction** (as compared to the average transaction amount and total account balance and/or monthly net income/revenue);
b. the **frequency, timing and pattern** of the same or similar transactions;
c. the **cumulative amount** resulting from the same or similar transactions (as compared to the average transaction amount and total account balance);
d. the **scope of the transaction**;
e. the **recipient of the transaction**;
f. any **relevant material public warnings on the recipient**;
g. other **inconsistent or exceptional nature of the transaction or series of transactions** as compared to the historical operation of the account.

ii. Financial Institutions, including Payment Institutions, licensed under the Financial Institutions Act

The provisions referred to earlier (in section (i) above for Banks and Credit Institutions), similarly apply to those payment service providers licensed under the Financial Institutions Act with whom the client has a payment account directly.

Financial institutions should be ready to defend complaints against them based on their merits and not rely entirely on the Arbiter's lack of competence to hear and adjudicate complaints against them on the basis of the complainant not being their eligible customer.

In particular, they should **adopt more robust onboarding procedures for corporate customers** that receive transfer of funds in their account from retail clients which carry the fingerprint of payments for investment services. Where their corporate clients receiving retail type funds happen to be involved in typical licensable activities, the financial institution needs to have **comfort that their corporate clients have proper onboarding systems for their own clients.** Furthermore, there must be **a convincing reason why corporate clients based in other jurisdictions involved in activities typically licensable sought account holding service with a Malta based financial institution.**

Where the fraud scheme involves a series of payments over a short period of time, the obligation for the institution to intervene at some point before continuing to process the payment, increases at each step of the way. Especially **when the payment order from the retail client gives only the IBAN number without clear identification of the beneficiary, the level of suspicion and need for investigation increases.**

iii. 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[11] 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),[12] for the devise of enhanced mechanisms to mitigate the occurrence of customers falling victims to such scams.

Furthermore, in the Arbiter's decisions of recent months there is a recommendation that VASPs should enhance their on-boarding processes where retail customers are concerned warning them that custodial wallets may be used by scammers promoting get-rich-quick schemes as a route to empty the bank accounts of retail customers and disappear such funds in the complex web of blockchain anonymous transactions.[13]

Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications.

VASPs are reminded that whilst their license under the VFA Act does not oblige them to adopt payments transactions monitoring mechanism as the PSD2 rules imposed on banks and credit institutions, Article 27(2) of the VFA Act obliges

---

[11] *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
[12] *Such as Case ASF 158/2021*
[13] *Such as Case ASF 069/2024*

them to the same fiduciary obligations as established in the Civil Code, in so far as they are applicable.

The lack of past long term relationship records does not readily offer them the possibility, as generally available to banks, to note patterns out of norm to their historical trends. But **if within the short-term span of transaction records, there are certain payments which are out of norm with the rest of the records, or if the transactions leading to the fraud are out of character with the KYC profile on the basis of which the customer was onboarded, the general fiduciary obligations should call for proper investigations and timely conversation with the client to warn against the possibility of fraud scams.**

For example, a payment for an amount which is evidently higher than other payments could be indicative of the fraudsters doubling down on their pig butchering attempts on the client (as was seen in cases where clients were demanded payment by the scammer equivalent to the supposedly accumulated profits for 'strict identification' excuses, with a fake promise to return the payment and profits).

F. Conclusion

It is in the interest of the industry to go the extra mile, even beyond regulatory requirements to ensure that consumers' confidence in the financial system is not eroded by the ease with which they perceive being tricked by fraudsters without proper protection from financial service providers.

The adjudication awards decided by the Arbiter will reflect the obligation of fairness, reasonableness and equity demanded by the Act through proceedings held informally and expeditiously but will also reflect the push that institutions need to invest in upgrading their monitoring systems in the interest of keeping a safe payments infrastructure.

The decisions on pig butchering fraud cases issued concurrently with these Technical Notes adopt a more lenient assessment of the transaction monitoring obligations of licensed institutions than would be adopted in future once the institutions have the benefit of considering, absorbing and adopting these Guidance Notes.

Consumers are also reminded to exercise caution, be careful in their dealings and stay aware of the specific risks associated with crypto-assets. In December 2024, the European Securities and Markets Authority (ESMA) issued additional warnings about crypto-assets, which consumers are urged to consider thoroughly.[14]

Consumers, especially retail type, should always bear in mind the maxim that if something is too good to be true, then, probably it is.

G. Annex

Summary of a few typical scenarios scammers use to trap victims in scams:[15]

i. Investment scams

Scammers use convincing marketing and new technology to make their investment sound too good to miss. They promise you big payouts with little or no risk. They often use pressure tactics to get you to act fast, so they can steal your money.

ii. Jobs and employment scams

Scammers offer jobs that pay well with little effort. They pretend to be hiring on behalf of high-profile companies and online shopping platforms. Sometimes, the job they list does not even exist. Scammers also impersonate well-known recruitment agencies. Their goal is to steal your money and personal information. They may ask you to pay money upfront to be able to work for them.

[14] https://www.esma.europa.eu/sites/default/files/2024-12/ESMA35-1872330276-1971_Warning_on_crypto-assets.pdf

[15] *Source: https://www.scamwatch.gov.au and other general websites*

iii. Products and services scams

Scammers pose as buyers or sellers to steal your money. They set up fake websites or profiles on legitimate retailer sites offering products or services at prices that are too good to be true. They post fake ads and fake reviews. They may use stolen logos and domain names making such scams hard to spot. Scammers also pose as businesses that you know and trust to send you fake bills. They can even change details on legitimate invoices so that customers end up paying the scammer instead of you.

iv. Romance scams

Scammers use the promise of love, dating, or friendship to get your money. They go to great lengths to convince you the relationship is real and manipulate you to give them money. Scammers find you on social media, dating or gaming apps and websites. They might also text or email you. They hide behind fake profiles and identities, sometimes of famous people.

Once you trust them, they will have an 'emergency' and ask for your help. This will often be requests for money or other products.

v. Threats and extortion scams

Scammers pretend to be from a trusted organisation and claim you need to pay money or something bad will happen. They may threaten you with arrest, deportation, or even physical harm, if you do not agree to pay them immediately. They can also blackmail you by threatening to share naked pictures or videos you have sent them unless you send them money.

vi. Unexpected money scams

Scammers try to convince you that you are owed or entitled to money or winnings that you did not expect to receive. The scammer asks you to pay a fee or to give your banking or identity details before you can collect the money or winnings. Unfortunately, there is no free money.

vii. Recovery scams

Victims of scams are often approached again by the scammer under a different guise (with the scammer possibly impersonating the police, a person of authority or an asset recovery company). Victims can also be cold-called by other scammers (who would have obtained a list of crypto victims), with such scammers promising and pretending to be there to assist them in recovering their stolen assets. A victim may also end up following an advert on social media by a fake crypto recovery service. Instead of recovering their assets, the victim ends up being duped again, losing more money in the process. The sophistication of such scams can vary, with the scammer even creating official websites purporting to provide asset recovery services that look legitimate but are fake.

ARBITER FOR FINANCIAL SERVICES

Issued: February 2025