ARBITER FOR FINANCIAL SERVICES

Technical NOTE

Follow-up to the Technical Note of February 2025 relating to 'Pig Butchering' Type of Scams

Contents

A. BACKGROUND 03

B. OUTCOME OF THE APPEALED CASE 04

C. ADDITIONAL INSIGHT INTO GOOD PRACTICES 05

1. Training of Staff and Education of Consumers 05

2. Other Internal Preventive Measures 08

3. Awareness of Use of Crypto-Assets in Fraud Cases 09

4. Customer Support and Redress - Proactive engagement and compassion 10

5. Other Important Developments 11

D. CONCLUSION 11

A. Background

This is a follow-up to the Technical Note of February 2025 regarding Relationship-Based Financial Fraud, also known as *'pig butchering scams'*, to provide additional feedback and updates relevant to cases involving such type of scams.

Relationship-Based Financial Fraud can have a devastating and significant impact, both financial and emotional, on victims of such fraud. This is an area of particular concern, which, together with other cases of financial fraud, has prompted the Arbiter to issue communications to the financial services industry with guidance on the considerations the Arbiter will take into account in determining complaints in this area.

This follow-up note is aimed for payment service providers (PSPs) - that is, banks and credit institutions licensed under the Banking Act[1] as well as financial and payment institutions licensed under the Financial Institutions Act[2]. It follows and takes into account important developments occurring since the issuance of the Technical Note of February 2025, namely:

i) **The outcome of the appeal filed before the Court of Appeal (Inferior Jurisdiction) to the Arbiter's decision in Case ASF 025/2024.**[3] This was one of the first cases involving pig butchering scams decided by the Arbiter at the start of 2025 based on the considerations outlined in the aforementioned Technical Note.

ii) **Additional cases** which the Office of the Arbiter for Financial Services ('OAFS') has been processing as complaints filed by consumers of financial services.

iii) **Recent relevant industry reviews and reports** considered of interest to PSPs with respect to fraud.

[1] *CAP. 371*

[2] *CAP. 376*

[3] *https://financialarbiter.org.mt/sites/default/files/oafs/decisions/1738/ASF%20025-2024%20-%20CL%20vs%20Bank%20of%20Valletta%20plc%20%28with%20Technical%20Note%29.pdf*

B. Outcome of the Appealed Case

The Court of Appeal's (Inferior Jurisdiction) decision of 19th November 2025 (Ref. 7/2025 LM)[4] is of particular relevance to the industry. The Arbiter's decision in Case ASF 025/2024 was confirmed, in its entirety, by the Court of Appeal, further validating the Arbiter's considerations and conclusion relating to the obligations of PSPs with respect to transaction monitoring and required reasonable intervention.

The Arbiter's decision for Case 025/2024[5] is now final and effective (res judicata) in terms of Article 27 of CAP 555.

In its decision of 19th November 2025, the Court of Appeal (Inferior Jurisdiction) referred to the provisions of *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market* ('the Payment Services Directive 2'), particularly article 68 sub-article (2) and (3) and its supporting framework,[6] and provided its interpretations in the context of the Arbiter's decision of the appealed case.

In reviewing new cases involving Relationship-Based Financial Fraud, the Arbiter will take into consideration the clear direction provided by the Court of Appeal in its decision of 19th November 2025 (Ref. 7/2025 LM).

[4] https://ecourts.gov.mt/onlineservices/Judgements

[5] https://financialarbiter.org.mt/sites/default/files/oafs/decisions/1738/ASF%20025-2024%20-%20CL%20vs%20Bank%20of%20Valletta%20plc%20%28with%20Technical%20Note%29.pdf

[6] *Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication. Preamble 2, Articles 2(1) and 2(2) of the Commission Delegated Regulation (EU) 2018/389 particularly featured in the decisions.*

C. Additional Insight Into Good Practices

This section outlines further good practices and areas for improvement which the Arbiter has observed from other cases of pig butchering scams considered throughout 2025,[7] new cases the OAFS has been approached with during this period, as well as from recent industry reviews and reports.[8]

The following are **four main areas identified** by the Arbiter **where PSPs are encouraged to implement and take stronger and more effective measures to combat the rising number of financial fraud cases:**

1) **Training of staff and education of consumers**
2) **Other Internal Preventive Measures**
3) **Awareness of role of crypto-assets in fraud cases**
4) **Customer Support and Redress**

Further background about each area is provided below. Where reference is made to specific cases decided by the Arbiter, a copy of the decision may be downloaded from the OAFS's website.[9]

1. Training of Staff and Education of Consumers

Well-trained and skilled staff can make a tangible difference in the prevention and timely response to financial fraud.

The **need for immediate specialist training of PSPs representatives, at both the contact centres and branch offices,** was highlighted by the Arbiter in various of his

[7] *E.g.: Case ASF 025/2024; ASF 122/2024; ASF 085/2024; ASF 204/2024; ASF 052/2025 amongst others.*

[8] *Such as the FCA's Multi-Firm Review titled 'Combating romance fraud – prevention, detection and supporting victims' published on 17th October 2025 - https://www.fca.org.uk/publications/multi-firm-reviews/combating-romance-fraud-prevention-detection-and-supporting-victims*

[9] *https://www.financialarbiter.org.mt/oafs/decisions*

recent cases.[10] Such focused training needs to enhance the competence and skills of the PSPs staff in identifying potential fraud and taking the necessary measures to safeguard potential victims.

The Arbiter recognises the difficulties that PSPs face in combating this area, given that victims of a scam may, as often directed by the scammers, hide or conceal certain information from the payment provider, including the true purpose of their payment transaction, which makes it harder for staff to suspect a scam.

Various instances, however, were noted by the Arbiter in which **the PSPs staff missed clear opportunities to spot a scam.** These are a few examples of such particular instances and red flags encountered in some of the cases considered by the Arbiter:

1.1 Customer calling the PSP to effect a material **increase in the transaction limit and/or the daily withdrawal limit,** with the limits being raised by the payment service provider **without clear and sufficient details and sight of the exact scope, nature and the extent of payments intended to be actually carried out to the same beneficiaries.**

Providing general and very basic explanations for increases in daily or transaction limits for substantial payments to be made needs to be considered more carefully and critically by trained staff. An introductory explanation that certain questions that may appear intrusive are meant to protect against fraud is often all that is needed to obtain customers' co-operation.

1.2 Customer making **multiple requests over a short period of time to raise the daily limit.**

A series of requests to enable multiple substantial payments is a clear red flag. For example, in Case ASF 122/2024, the Complainant called her bank three times over a week to increase her account limits.

1.3 **Frequent/substantial anomalous payments to the same beneficiary and/or third-party transfers,** including to one's own personal account held with another third-party provider.

[10] *Example: Case ASF 204/2024 and ASF 052/2025*

In Case ASF 122/2024, for example, the Complainant made various substantial transfers over a few days to her own bank account held with another overseas third-party provider. A similar pattern also emerged in Case ASF 085/2024 when successive significant payments were made over a very short amount of time to the Complainant's personal account similarly to an overseas third-party provider.

1.4 **Queries or communication of intended large inward transfers** of money into the customer's accounts is another potential indicator of the manipulation of the victim, who would be deceived by the fraudster into believing that a transfer of the alleged substantial fictitious profits would occur (as has happened in Case ASF 122/2024).

1.5 **Outward substantial payments attempted by the victim through various means,** not just through online payments but also through cash withdrawals.

More effective and continuous specialist training (including on current and prevalent scams), is an important tool that equips the PSP with the ability to spot such scams at an early stage and provide for a timely intervention to prevent the perpetration of a scam and limit customers' losses.

Staff need to be trained to spot abnormal patterns in payment history that require intervention. Each case is different, and whilst a pattern may appear quickly in just one or a few days, in some cases it can develop over several weeks or months.

The Arbiter appreciates that more intrusive questions and the need for PSPs staff to probe further, potentially even pausing or blocking transactions in justifiable circumstances where a scam is suspected, may not be welcomed and resisted by a consumer. Staff need to:

- skilfully and professionally obtain relevant information and critically review and reasonably question the explanations provided by the consumer where necessary;
- better understand fraud scenarios and a victim's frame of mind when under the manipulation of a fraudster;
- determine what appropriate actions are necessitated in the particular circumstance presented before them.

The aim remains to ultimately:

- **achieve the right balance and take proportionate measures in the consumer's interest.** This can be achieved through specialist training and current internal procedures reflective of the fraud scenarios being experienced in today's financial industry, and
- **educate customers to alert them about new scam scenarios** and the need for them to be vigilant, and on how to protect themselves, is another key preventive area.

The Arbiter positively acknowledges the enhanced efforts being taken, including frequent SMS alerts, various podcasts, TV and radio appearances, and even moving billboards on buses to increase awareness of scams. Ongoing educational initiatives are encouraged and commended. The use of real-life examples about the risks of investing through unknown or unlicensed contacts obtained from social media, online relationships and online financial requests is particularly useful to create and raise awareness of the dangers posed to consumers.

2. Other Internal Preventive Measures

The Arbiter notes that the FCA's recent review on combating romance fraud identified useful practices worth highlighting.[11] Various of the incidents highlighted in the said review were commonly and similarly seen in cases filed with the OAFS.

The following are additional examples of good practice identified in the said FCA's report, which the Arbiter will also take into consideration for future cases of pig butchering scams:

2.1 **Marker of a vulnerable client and enhanced sensitivity and monitoring for such customers,** in the instance where the payment provider is aware or alerted to the vulnerability of a customer.

[11] https://www.fca.org.uk/publications/multi-firm-reviews/combating-romance-fraud-prevention-detection-and-supporting-victims

[12] *Refer for example to recent decision re case ASF 204/2024*

2.2 **High-risk payments paused or deferred for manual intervention,** with the payments temporarily blocked in order for the customer to be required to first interact with the PSP representative before the payment can proceed. This applies particularly to payments to new beneficiaries.

2.3 **Borrowed funds from family members, friends or sale of personal assets with the intention to be immediately transferred to another beneficiary** should also trigger alerts for further investigation.

Other good practices identified by the Arbiter during his interactions with local institutions include:

2.4 **Introduction of pause periods:** following approval of increased spending limits as may be merited in certain circumstances (such as adjustments to limits made remotely); following a questionable change of registered devices.

2.5 **Introduction of alert pop-ups** in the case of online payments, counselling a **re-check by the payer of the integrity of the beneficiary** before releasing payments.

3. Awareness of Use of Crypto-Assets in Fraud Cases

Many fraudulent scams involving relationship-based fraud (pig butchering) result in digital assets being sent from crypto exchanges to external wallets on blockchain where the identity of the recipient is hard to prove. In most cases these transfers are authorised by the victims in search of illusionary gains, before they realise that they were being duped by the scammers.

As some banks question and/or block direct payments to crypto exchanges, scammers may instead direct victims to transfer funds to an intermediary PSP (other non-bank financial institutions). Victims are guided by the scammers to name themselves as beneficiaries, but quote accounts to be credited (such as Virtual IBANS) belonging to the crypto exchange or other crypto-related merchant that holds an account with the intermediary PSP.

In this manner, transfer of funds which could normally be questioned or blocked by the victim's traditional bank would find themselves on a crypto account of the victim

(normally opened under the guidance of the scammer), where the funds are then converted to crypto-assets and eventually transferred to the fraudulent external wallets.

PSPs handling such a transfer of funds should be suspicious when they receive funds from retail/personal clients naming themselves as beneficiaries (even though they would hold no account with the PSP) whilst quoting account numbers of the crypto merchant.

This pattern is so prevalent in various cases seen by the Arbiter that PSPs are expected to suspect fraud and revert to the remitter bank to correct the identity of the named beneficiary before proceeding with crediting the proceeds to a beneficiary different from the one named in the transfer order.

4. Customer Support and Redress - Proactive engagement and compassion

The support afforded to victims appeared somewhat lacking in the cases seen, with at times, no proactive or limited interaction held by the PSP with the victim.

In Case ASF 085/2024, for example, the customer highlighted that despite the severity of her claim (where she lost around EUR 70,000), the bank's fraud team never contacted her directly about her case.

The Arbiter considers it in the PSPs interest to engage the customer in an active discussion to gather relevant information and assess emerging trends in scams, also as part of developing a strong internal investigative practice.

It is likewise important for the payment service provider to demonstrate empathy rather than a dismissive attitude towards its customers. **This calls for a cultural shift towards a customer-centric approach rather than a defensive one, with a greater focus on consumer protection and commitment towards the customer.**

Such empathy also appears missing when PSPs keep appealing cases where the Arbiter finds fault and awards compensation to victims, even where similar decisions have been already appealed and denied by the Court.

5. Other Important Developments

Compliance with the requirements regarding instant credit transfers brought by 9th October 2025, under the Instant Payments Regulation (IPR), also needs to be duly taken into consideration.[13] Important aspects in this regard include the service of payee verification for fraud prevention and potential implications related to the adjustment of spending limits by the Payment Service User (PSU).

The Arbiter acknowledges and supports the adoption of a risk-based approach with respect to the PSU's adjustment in spending limits, with reference to the 'Notice on the Introduction of a Delay Period for Instant Credit Transfers', issued by the Central Bank of Malta on 17th September 2025.[14] Reference is also made to the document issued by the Financial Intelligence Analysis Unit (FIAU), in collaboration with the Central Bank of Malta, in December 2025 titled *'Clarifications on AML/CFT issues under Regulation (EU) 2024/886 (IPR)'*.[15]

D. Conclusion

The proliferation of pig butchering scams has continued to increase over the past years, as evidenced by the rise in complaints from victims and widespread media coverage worldwide.

In its report of October 2025, titled *'ENISA Threat Landscape 2025'*, the European Union Agency for Cybersecurity (ENISA) *inter alia* reported that:

[13] *Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro.*

[14] https://www.centralbankmalta.org/en/news/14/2025/11300

[15] https://fiaumalta.org/news/new-qa-document-aml-cft-clarifications-under-regulation-eu-2024-886-ipr/

'Observed since at least the mid-2010s in China and globally since 2019[201], pig-butchering scams[202] are increasingly reported as being leveraged to target citizens in EU MSs. In 2024, pig-butchering scams grew by almost 40% year-on-year, reportedly generating between €9.1 (USD 10.6) billion and €11.4 (USD 13.3) billion, and accounting for over one-third of global cryptocurrency scam revenue[203]. Throughout this period, open sources noted the increased use of generative AI and deepfake videos to impersonate trusted contacts, enhancing the social-engineering phase of these scams.' [16]

Original Source References

[201] https://www.scmp.com/news/people-culture/social-welfare/article/3150688/online-pig-butchering-love-scams-have-gone

[202] *Scams in which threat actors spend weeks or months building trust with victims, often through fake online relationships, before defrauding them of their money, often by convincing them to invest in fraudulent cryptocurrency platforms.*

[203] https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/

The European Banking Authority (EBA) described payment fraud as *"still the most significant issue for EU consumers as a result of new types of fraud such as 'Authorised Push Payment' (APP) fraud, where the payer is manipulated into making a payment to the fraudster'"*, as outlined in its report titled *'EBA Consumer Trends Report 2024/25 of 26 March 2025'*.[17] Furthermore, in its recent report of December 2025 relating to payment fraud, the EBA reported an increase in fraudulent payments, noting that *'The total value of fraudulent payment transactions reported by the industry across the European Economic Area (EEA) amounted to EUR 4.2 billion in 2024. This represents a year-on-year increase of EUR 602 million or 17% from 2023 to 2024'*.[18]

The local financial sector and consumers are not immune from this increase in fraud. During 2025, the Office of the Arbiter for Financial Services was approached by complainants who had suffered significant losses from pig butchering scams ranging from low five digit to high six digit figures.

---

[16] *P. 32 – 33 of the 'ENISA Threat Landscape 2025' report dated October 2025 -* https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf

[17] *P. 7 of the EBA Report (EBA/Rep/2025/08) -* https://www.eba.europa.eu/sites/default/files/2025-03/514b651f-091b-42d3-b738-1fae79264044/Consumer%20Trends%20Report%202024-2025.pdf

[18] *Page 10 of the '2025 Report on Payment Fraud' (EBA/Rep/2025/40), December 2025 -* https://www.eba.europa.eu/sites/default/files/2025-12/1709846a-84d9-47cf-86a0-b155efb34d66/EBA%20and%20ECB%20Report%20on%20Payment%20Fraud.pdf

As outlined in a recent article in the local media, *'Reports to the police about investment scams, romance scams and similar frauds have gone up a lot in recent years' where 'the police are receiving an average of 15 reports about online scams every day'*.[19] The true extent of such scams is likely to be underreported, given the embarrassment and helplessness many victims feel.

Good industry practice shows that, in general, PSPs do intervene as they indeed should.

The Arbiter appreciates that local PSPs prevent many financial scams through the use of automated IT systems implemented over the past years and their proper and timely interventions to tackle fraud. PSPs are, however, encouraged to review and strengthen certain aspects of their internal systems to continue combating fraud effectively. In particular these have to take account of the following points:

1. The bar for payment institutions claiming gross negligence on the part of victims is tending higher as fraud cases grow exponentially and scamming is becoming a creative and lucrative criminal industry.
2. While scammers adopt AI as an effective instrument for their trade, PSPs should adopt AI to enhance their payments monitoring mechanism with effective real time controls.
3. Matching IBANs and, where applicable Virtual IBANs, to indicated payee is an ever more effective tool to detect and stop fraud.

The Arbiter will, in the meantime, continue to follow closely the developments currently under consideration at the EU level with respect to the PSD legislative framework.

Industry associations are furthermore encouraged to work closely with law enforcement and regulatory authorities to enhance and devise mechanisms on how they can work together to reduce and tackle these evolving scams.

[19] *Times of Malta article dated 28th September 2025 - https://timesofmalta.com/article/watch-i-impersonating-mother-scammer-save-her.1116952*

ARBITER FOR FINANCIAL SERVICES

Issued: January 2026

financialarbiter.org.mt