ARBITER FOR FINANCIAL SERVICES

NEWSLETTER

Issue 6 (December 2025)

Contents:

A WORD FROM THE ARBITER

Alfred Mifsud, Arbiter for Financial Services

Decisions

During 2025, 125 decisions were issued compared to 94 and 137 in the same period of 2024 and 2023, respectively.

In addition, during the period there were another 65 cases that were closed without adjudication. These were complaints against a common service provider that was forced into liquidation through regulatory action by the MFSA.

Sector	2023	2024	2025
Banking / Payments	31	31	51
Corporate Services	0	3	0
Insurance	31	31	33
Investments	75	29	41
Total	**137**	**94**	**125**

Fifty-four of the 125 decisions related to complaints registered in 2025. Seventy decisions related to complaints filed in 2024 and one decision to a complaint that was filed in 2023.

As at end of December 2025, there were only two cases pending that were registered in 2024 which were still active awaiting adjudication. These were complex cases requiring extensive evidence gathering and we expect to issue final adjudication in the first quarter of 2026.

The 125 decisions resulted in five complaints being fully upheld, 38 cases being partially upheld and 82 cases not being upheld (for various reasons, including the merits of the case, lack of competence, legal issues and a single case where the complaint was considered frivolous). In total, compensation amounting to around €286,000 was awarded to complainants in cases that were fully or partially upheld.

We have far exceeded the decision output of 2024 though we are still below the 2023 level. The 2023 record output was due to a backlog of decisions brought forward from 2022 when only 72 decisions were issued. There are at present only a handful of cases pending merely awaiting decisions and these will be formally adjudicated in the first months of 2026.

Appeals

Twelve decisions were appealed. Of these, one was withdrawn and one was decided confirming the decision of the OAFS. Ten appeals are still pending:

- 1 case in which the complaint was fully upheld – appealed by the service providers;
- 6 cases that were partially upheld – appealed by the service providers;
- 1 case where the Arbiter declared non-competence – appealed by the complainant;
- 1 case declared frivolous – appealed by the complainant; and
- 3 cases not upheld – 2 cases appealed by the complainant and 1 case by the service provider.

Five cases appealed in prior years were closed during 2025. One appeal was withdrawn and four appeals largely confirmed the Arbiter's decisions.

We regret that banks and financial institutions continue to appeal decisions taken in which full or partial compensation was awarded.

Where the Arbiter's decision is confirmed on appeal, we expect such decisions to be considered final without appeal of decisions with similar circumstances. Such appeals merely delay the payment of compensation due to complainants, often victims of fraud scams.

New complaints

Over 330 new complaints were registered in 2025 compared to 151, 224 and 251 in the three years 2022-2024. This is the highest number of complaints filed since the Arbiter's Office was established in 2016. The significant increase reflects the explosion of fraud complaints based on crypto fraud.

These complaints were filed against:

- **banks** who are expected to spot and stall such scams;
- **non-bank payment service providers** whose systems are used by scammers to convert identifiable fiat funds into untraceable crypto assets; and
- **crypto exchanges** (Crypto Asset Service Providers – CASPs) who transfer crypto assets to fraudulent wallets, as victims duped by illusionary quick profits, allow themselves to be manipulated by scammers.

Very few of these fraudulent cases are being settled through mediation since licenced institutions are inflexibly denying any responsibility and it takes decisions issued by the Arbiter, being confirmed on appeal, for quicker outcomes to filter through the mediation settlements.

Going forward

We are issuing several guidance papers to explain our expectation on the conduct of licenced institutions insofar as scam experiences. It is in the interest of the industry to do whatever needs to be done to build systems capable of spotting and investigating suspicions of fraud before scammers disappear with the money. Such scamming has reached a significant industrial magnitude on an international level.

Unless institutions invest in modern technology, including AI, to gain effective tools to prevent these scams, there is a grave risk of people losing faith in the financial system and resorting to crypto payments, which awkwardly is the main hosting venue for such scams.

Decisions in the pipeline for 2026 will set precedents for responsibility for such scams by non-bank PSPs and CASPs now that the MICA legislation became effective in 2025, increasing the transaction monitoring obligations to the same level as for credit institutions under the PSD2. However it must be emphasised that consumers should bear in mind that protection is better than cure. **The only ones who can make easy, quick gains are the scammers at the expense of innocent, gullible victims.**

ARBITER FOR FINANCIAL SERVICES

LINKEDIN POSTS

In our weekly LinkedIn posts, we typically feature a decision of the Arbiter for Financial Services that focuses on a particular issue or area. The focus has now evolved to include lessons learned for financial services providers, with relevant questions posed to directors and compliance officers.

Arbiter dismisses crypto investment scam case

A university economics professor lost €41,000 through a cryptocurrency scam involving multiple service providers. The Arbiter dismissed complaints against three entities, ruling the complainant's gross negligence caused the complainant's losses, not regulatory failures. Case ASF 228/2024 was decided on 18 August 2025.

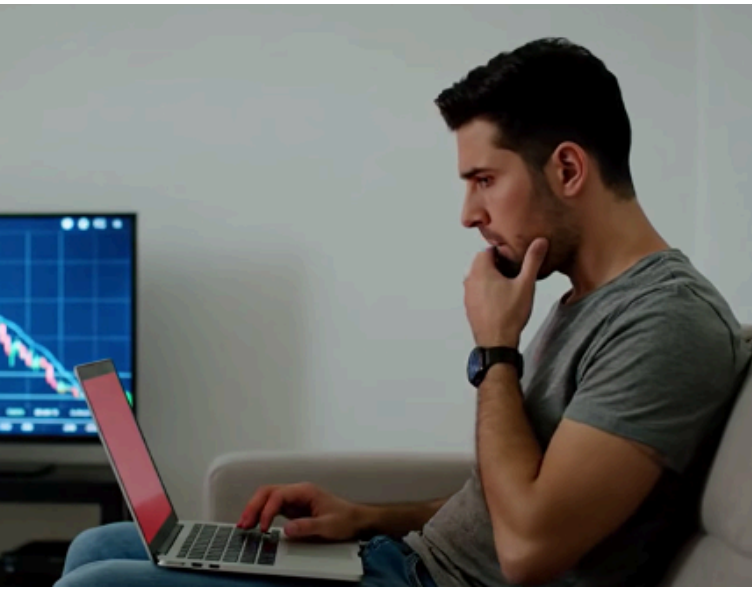
The Complaint: The complainant fell victim to a scam orchestrated through platforms initially called 'Entricapital', later 'lloy-dsb', which claimed association with Lloyds Bank UK. Between July and September 2024, he transferred €148,990 to fraudsters, who promised substantial investment returns. The complaint to the Arbiter concerned €41,000 transferred through three Malta-licensed providers: €28,500 through Financial Institution 1 (FI1), which then passed the funds to another financial institution (FI2). These were converted to cryptocurrency and transferred to the complainant's wallet with a crypto asset provider, from where they were sent to external wallets controlled by fraudsters. The complainant admitted to installing remote access software and giving scammers full access to his accounts. He sought compensation totalling €71,100, including interest and consequential losses.

Service Providers' Responses: FI2 stated that it followed the complainant's instructions after identity checks and confirmations. It stated that it issued warnings before each transaction about scams and irreversibility. It also stated that its systems showed no link between recipient addresses and known fraud. FI1 initially challenged the Arbiter's jurisdiction, arguing the complainant was not their eligible customer. After this preliminary plea was dismissed, they explained their use of Virtual IBANs and their role as intermediary.

Arbiter's Analysis: The Arbiter addressed each service provider separately, recognising their different regulatory obligations. For FI2, the evidence showed they acted solely as instructed by the complainant, with no involvement in diverting funds. For the crypto asset provider, the Arbiter examined applicable regulatory frameworks, including the Virtual Financial Assets Act 2018 and associated regulations. While acknowledging the complainant fell victim to a scam, the Arbiter found no breach of specific obligations or regulatory requirements. The cryptocurrency transactions, once processed, could not be reversed as warned in the service terms. Critically, the complainant confirmed knowingly granting fraudsters access to his accounts and that he understood transfers through FI1 were transit mechanisms, not destinations. For FI1, although the Arbiter identified a regulatory breach in crediting funds to Virtual IBAN (VIBAN) account holders rather than named beneficiaries, he found no direct causation between this failure and the complainant's losses. The complainant's admission that he knew he was naming himself as beneficiary while understanding the money would reach fraudsters proved determining.

The Decision: The Arbiter dismissed all three complaints. The Arbiter distinguished this case from ASF 155/2024 (involving FI1), where a vulnerable elderly victim succeeded. Here, the complainant was an economics professor who clearly understood the transaction mechanisms. His continued transfers, despite receiving explicit warnings from his Italian bank about 'false trading', demonstrated gross negligence that caused his losses, not regulatory failures by the service providers. The Arbiter directed that FI1's conduct regarding VIBANs be reported to the Malta Financial Services Authority for regulatory investigation but found this breach did not cause the complainant's losses.

CFD Trading appropriateness assessment failure results in compensation award



The Arbiter for Financial Services ruled in favour of a complainant who lost €13,000 trading CFDs (Contracts for Difference) – complex financial products – through an online platform. Case ASF 081/2025 was decided on 18 August 2025. The complainant argued that high rollover costs and the ease with which money could be lost constituted a scam-like operation.

An Italian retail client deposited €13,000 over four months to trade CFDs but lost nearly all funds through trading losses and fees. The complainant questioned the service provider's regulatory status and contractual relationship validity, suspecting collusion with an educational platform. They claimed excessive rollover costs facilitated rapid capital depletion and sought full reimbursement.

The service provider maintained full regulatory compliance as a Malta-licensed investment firm operating under MiFID II. They argued they operated as a straight-through-processing CFD broker without proprietary trading or client fund investment. The provider denied any affiliation with third parties and insisted all fees were transparently disclosed. They claimed the complainant underwent proper onboarding and appropriateness assessments (when your service provider is taking you on as a client for the first time).

The Arbiter identified material shortfalls in the appropriateness assessment process. Despite the complainant indicating low income (under €20,000 annually), basic education, no relevant experience and misunderstanding CFD risks, the provider proceeded with onboarding. The complainant incorrectly described CFD trading as "safe with very low risk" and sought "medium-low risk" exposure, contradicting CFD characteristics. These red flags should have triggered intervention to protect this vulnerable client.

The Arbiter awarded €6,350 compensation (50% of net losses) plus 2.15% annual interest, finding the service provider's appropriateness assessment failures enabled the significant losses while acknowledging the complainant's contributory responsibility for ignoring risk warnings.

When cryptocurrency investment scams meet banking obligations: Lessons from a "pig butchering" scam

A 72-year-old complainant fell victim to a cryptocurrency investment scam, losing €28,918 through some 70 transactions over six weeks. Case ASF 246/2024 was decided on 28 August 2025, with the complainant seeking full reimbursement from their bank for failing to detect and prevent the fraudulent scheme.

The complainant argued that their bank should have recognised the unusual pattern of frequent payments to a fintech account as suspicious activity. They contended that the bank had a duty to intervene when payments became abnormally frequent, particularly given their age and vulnerability to such scams. The complainant maintained they were acting under duress from scammers who had convinced them to invest in Bitcoin through increasingly sophisticated manipulation techniques.

The bank argued in its defence that all transactions were properly authorised using strong customer authentication methods, including 3D Secure and push notifications. They emphasised that payments went to the complainant's own fintech account, making them appear legitimate. The bank highlighted their transaction monitoring systems, which assessed these payments as low risk, and noted that the complainant had not disclosed the true purpose of the transfers when making enquiries about a suspicious payment.

The Arbiter examined whether the bank's transaction monitoring obligations were met, recognising this as a typical "pig butchering" scam. While acknowledging the payment pattern was anomalous compared to the account's previous activity, the Arbiter found the individual amounts were relatively small and the total not extraordinarily suspicious for someone with a working income.

The analysis revealed the complainant had multiple opportunities to disclose the fraud but chose to conceal information, including about fake correspondence and a non-existent €4,600 payment that supposedly arrived but never materialised.

The Arbiter rejected the complaint, concluding that the complainant bore full responsibility for the loss, having ignored clear fraud indicators and failed to be truthful with the bank when opportunities arose to prevent further losses. Both parties were to bear their own costs. Read the full decision at this link: https://shorturl.at/8oPxL.

Arbiter rulings on estimated maturity values

Two complaints (ASF 007/2025 and ASF 042/2025) were decided on 18 August 2025; both alleged that the maturity sums offered at policy maturity were materially lower than the 'Estimated Maturity Value' shown at sale.

The first case involved a couple who purchased a life policy in 2000, claiming the representative guaranteed €23,473 at maturity after 25 years of premiums. The second case featured a policyholder who bought an endowment policy in 1994, alleging the representative assured him of receiving €71,586 after 30 years, based on estimated maturity values.

The provider replied that the figures in the quotations were estimates based on then-current bonus rates, that reversionary/terminal bonuses were declared at its discretion and were not guaranteed, and that policy documents and annual statements had explained this.

The Arbiter examined the quotations, Important Notes, product information and policy schedules, and found that the estimated maturity figures were not guaranteed and had to be read in context. He acknowledged, however, that some expectations were reasonable and that a single-point quotation could have been misleading over multi-decade terms. The policies still provided life cover and achieved positive returns of 3.6% and 4.2%, respectively.

In ASF 007/2025, the Arbiter accepted the complaint in part, treated €27,426.24 as the final maturity figure for assessment and awarded limited equitable compensation. In ASF 042/2025, the Arbiter likewise found the complaint justified to a limited extent and quantified the fair remedy having regard to the documents and conduct.

Remedy: the Arbiter – acknowledging that expectations were not entirely unreasonable, given the sales presentations – awarded €4,114 in compensation in the first case and €1,496 in the second, plus the original maturity value. Procedural costs were assigned against the provider.

Read the full decisions at these two links: https://shorturl.at/yf1GU and https://shorturl.at/JvAw4.

Unauthorised investment switch

The Arbiter for Financial Services partially upheld a complaint about an unauthorised switch of an investment in a decision on 12 September 2025 (Case ASF 070/2025). The switch allegedly caused financial loss and stress to the complainant. The dispute centred on whether the service provider acted in the client's best interests and obtained proper consent.

The complainant invested €250,000 in a Malta government bond fund as part of their residence visa programme requirements in 2019. The complainant claimed that this investment was replaced without his knowledge or consent by another fund with a lock-in period. This change disrupted his financial plans, caused liquidity issues and led to losses when he needed early redemption. He argued that the service provider failed to notify him, verify authorisation validity and act in his best interest.

The service provider argued the complaint was time-barred and that it acted on valid instructions under a power of attorney granted to the complainant's lawyer. It maintained that all disclosures were made to the attorney, that the complainant later signed a full and final settlement agreement voluntarily, and that the switch aimed to enhance returns without increasing risk.

The Arbiter dismissed the time-bar plea, ruling that the relevant date was when the complainant personally became aware of the switch in 2025. He found material shortcomings in the provider's conduct: failure to obtain mandatory fund-specific declarations, reliance solely on internal forms, and lack of direct confirmation from the client for significant changes, including reclassification to professional status and a new lock-in period.

The Arbiter held that the provider did not act with due skill, care and diligence, nor in the client's best interests, as required by regulatory principles. The settlement agreement did not preclude claims related to the original investment.

The complaint was partially upheld. The provider was ordered to pay €10,000 plus interest at 2.15% p.a. from the decision date, reflecting the difference between the original investment value and the amount received after early redemption. Claims for moral damages were rejected.

Read the full decision, which is subject to appeal, at this link: https://shorturl.at/bkuKf.

What happens when Virtual IBANs meet weak controls? A recent Arbiter decision sheds light on compliance gaps that can cost reputations

Case ASF 016/2025 (31 October 2025) examined a complaint where a consumer lost €85,700 to investment scammers promising €10,000 monthly returns. Between May and July 2021, she made six transfers to what she believed was an account with a financial services provider, but funds actually went to an Estonian company operated by fraudsters.

The complainant alleged the provider failed proper AML/KYC checks, facilitating fraud. The provider contested competence, claiming no customer relationship existed. The Arbiter ruled that she was an "eligible customer" because she nominated the provider as the beneficiary bank on her transfers.

The service provider countered that the Arbiter lacked competence, arguing the complainant was not an "eligible customer" under Maltese law and that it relied on onboarding controls of an intermediary.

On the merits, the Arbiter acknowledged the provider improperly credited funds to a Virtual IBAN account holder rather than the named beneficiary – a breach that was referred to the Malta Financial Services Authority.

However, the complaint was dismissed since the complainant admitted knowing funds would reach the Estonian company, conducted only 'amateurish' due diligence and pursued unrealistic returns. The Arbiter found her losses stemmed from "greed and gross negligence", not the provider's regulatory failures, since no direct causation existed between the breach and her loss.

Lessons for Financial Services Providers

- Do not rely solely on intermediaries' AML/KYC checks. Ultimate responsibility for compliance rests with the licensed entity.
- Reliance on intermediaries' controls is not enough; boards must understand and oversee how virtual IBANs and merchants are handled in practice.
- Clear authority for fund redirection is essential. Crediting funds to an account other than the named beneficiary without explicit consent is a serious breach.

A few questions for directors and compliance officers

1. Are your onboarding and monitoring frameworks robust enough to detect high-risk arrangements like VIBANs?

2. How do you ensure reliance on third-party checks does not dilute your own regulatory obligations?

3. Have you stress-tested governance, risk and reporting frameworks around intermediaries and virtual IBANs, including when and how you escalate issues to regulatory authorities?

Download the full decision at this link https://shorturl.at/04uQE to review the Arbiter's detailed analysis of VIBAN regulatory gaps and consumer protection boundaries.

Appeal Court confirms bank's duty to monitor and act on suspicious transaction patterns

ARBITER FOR FINANCIAL SERVICES

On 19 November 2025, the Court of Appeal (Inferior Jurisdiction, case 7/2025) entirely confirmed a decision issued by the Arbiter for Financial Services early in 2025 in the case Arthur Bonnici v Bank of Valletta plc (ASF 025/2024).

Arthur Bonnici complained that Bank of Valletta plc (BOV) failed to intervene when he made unusual payments totalling €65,446.57 over seven months to cryptocurrency platforms.

He fell victim to a "pig butchering" scam in which fraudsters manipulated him into investing in crypto assets. While the complainant authorised all transactions himself, he argued the bank should have identified the suspicious pattern and intervened. BOV maintained it properly processed legitimately authorised payments and had no obligation to interfere with a client's investment choices.

The Arbiter found BOV failed its payment monitoring obligations. While acknowledging the complainant bore some responsibility, the Arbiter ordered BOV to refund €24,695.82 (payments made after 17 December 2022), concluding the bank should have initiated a conversation with the client about the anomalous transactions.

BOV appealed on two grounds, namely that it had no legal obligation to perform the extensive monitoring the Arbiter suggested, and that Payment Services Directive 2 only required intervention for unauthorised transactions, not legitimately authorised ones.

The Court of Appeal (Inferior Jurisdiction) confirmed the Arbiter's decision entirely. It emphasised that banks' monitoring responsibilities extend beyond individual transactions to encompass patterns viewed against historical account activity. The Court noted that 20 payments occurred within two months, 11 exceeding €2,000 (amounts never previously transacted), with cumulative amounts exceeding 150% of the client's declared annual salary by mid-December.

The Court stated these factors should have triggered direct client communication. The Court rejected the bank's 'tipping off' defence, noting banks routinely contact clients about unusual activity. The Court concluded that the bank's failure to communicate with its 20-year client, despite completely atypical transaction patterns, directly contributed to enabling the fraud.

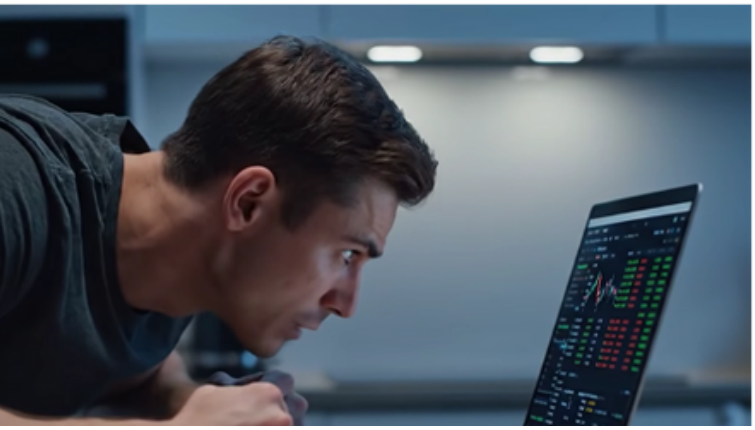
The Court rejected BOV's narrow interpretation of its obligations. It stated that Article 68(2) of PSD2 – which permits banks to block instruments for "objectively justified reasons relating to security" – must be interpreted broadly beyond mere identifying theft scenarios. The Court reasoned that, if banks must intervene when clients may lack means to repay credit, they equally must act when indicators suggest risky or potentially fraudulent movements with deposited funds.

Download the Arbiter's decision and the Court of Appeal Judgment from this link: https://lnkd.in/dAKNCQqm.

LESSONS LEARNED: LEVERAGING THE ARBITER'S DECISIONS FROM A CONSUMER PERSPECTIVE

Each week, in our Facebook post, we regularly feature lessons learned from decisions of the Arbiter for Financial Services and give advice in specific situations related to financial products. Apart from posting in English, we also post in Maltese.

Lessons for consumers from Arbiter's decision on online trading



A recent case showed how one investor lost almost all their savings within a few months of trading Contracts for Difference (CFDs) – complex financial products – online. The Arbiter found that, although the provider was regulated, it had failed to properly assess whether the client understood the risks. The client also carried part of the responsibility for ignoring clear warnings. In the end, compensation of half the losses was ordered.

Key lessons for everyday consumers:

1. Know the risks – Contracts for Difference (CFDs) are complex financial products. Most people lose money when trading them. If you don't fully understand them, don't invest.

2. Check your profile – If your income or savings are limited, these products can quickly wipe out your funds. Only use money you can truly afford to lose.

3. Be honest in assessments – When asked questions during onboarding (your service provider is taking you on as a client for the first time), give accurate answers. Wrong or careless replies can expose you to products that aren't suitable for you.

4. Don't rely on others blindly – If someone pushes you into trades, remember that the risks are yours alone. Always question advice from unverified "consultants" or websites.

5. Act on warnings – Risk disclosures are there for a reason. Read them carefully and take them seriously before depositing any money.

These lessons are based on the Arbiter's decision ASF 081/2025. You can read more about the decision here https://shorturl.at/jKtRz.

Consumer lessons from recent cryptocurrency scam cases

Based on the Arbiter's recent decisions in cases ASF 025/2025 and ASF 038/2025, two complainants lost €78,700 and €86,300, respectively, after falling victim to investment scams. Both had transferred funds from their bank accounts to a cryptocurrency platform, which were then sent to external wallets controlled by fraudsters.

The complainants argued the cryptocurrency platform should have detected irregular transactions and prevented the transfers. However, the Arbiter rejected both complaints, finding no evidence that the service provider breached its regulatory obligations. The decisions highlighted that consumers bear responsibility for transactions they personally authorise, even when deceived by scammers.

Key lessons for consumers:

1. You're responsible for your own transactions – Even if you're tricked by sophisticated fraudsters, cryptocurrency platforms aren't required to compensate you for transfers you personally authorised. The blockchain technology makes these transactions irreversible once completed.

2. Cryptocurrency isn't banking – Don't expect the same consumer protections you'd get from traditional banks. Virtual Financial Assets (VFA) providers operate under different regulations with fewer safeguards for customers.

3. Remote access software is a red flag – Be extremely wary if anyone asks you to install software like AnyDesk that gives them control of your computer or accounts. This is a common tactic used by scammers to maintain access to your funds.

4. Act quickly when suspicious – Contact service providers immediately when you suspect fraud. Waiting months after transactions are completed significantly weakens any potential claim for assistance.

Ready to learn more? Review the full decisions on the Office of the Arbiter for Financial Services website at these links – https://shorturl.at/DSJOs and https://shorturl.at/6FMNa.

Understanding trading platform responsibilities

A retail customer with six years of trading experience claimed losses of approximately €21,000 after migrating to a new trading platform. The customer alleged inadequate disclosure about hedging strategies, swap charges and platform usability issues that prevented timely deposits during margin calls.

After examining the evidence, the Arbiter dismissed the complaint entirely, finding that the service provider had fulfilled its regulatory obligations and that the customer, despite being classified as retail, possessed substantial trading experience and bore responsibility for understanding the risks of their chosen investment strategies.

Key lessons for consumers:

Lesson 1: Sign disclosure documents carefully

When you tick a box confirming you have read and understood risk disclosure statements, you accept responsibility for that knowledge. The Arbiter found the complainer executed over 4,000 trades before experiencing losses. So, he could not credibly claim ignorance of risks clearly outlined in the onboarding documents signed years earlier.

Lesson 2: Experience matters more than classification

While you may be classified as a 'retail customer' entitled to certain protections, your trading history speaks volumes. Regular trading activity (in this case, over 2,000 trades annually) demonstrates practical knowledge. The courts will consider this when assessing whether you genuinely did not understand the risks involved.

Lesson 3: Service providers are counterparties, not advisers

Unless specifically licensed to provide investment advice, trading platforms act solely as counterparties to your transactions. They are not required to recommend when to hedge positions or advise on trading strategies, even if customer service representatives discuss your approach with you.

Lesson 4: Margin calls require proactive management

If your account reaches margin call status, you bear responsibility for meeting those calls promptly using available deposit methods. When you have 10 days' notice but attempt a last-minute deposit late at night and then blame technical difficulties, you will not persuade an Arbiter that the provider failed in its duties.

Lesson 5: Platform familiarity is your responsibility

Executing hundreds of trades on a new platform before experiencing problems demonstrates you understood how it worked. Claims of inadequate training or platform deficiencies carry little weight when you have already successfully navigated the system numerous times.

Lesson 6: User errors are not provider failures

Technical issues that result from missing mandatory steps (such as selecting account currency during deposits) constitute user error rather than platform malfunction. This is particularly so when no other customers report similar problems, and you subsequently complete transactions successfully using the same method.

Want to learn more? Review the full decision at this link https://shorturl.at/pisXk to understand how trading experience, disclosure obligations and customer responsibilities interact in financial disputes.

Early pension exit costs: The documents consumers cannot ignore

A consumer disputed an early redemption/surrender fee of c. £12,000 deducted when exiting a pension arranged via a platform within a QROPS (Qualifying Recognised Overseas Pension Scheme). The Arbiter held the complaint was in time but found the signed platform application and tariff schedule clearly provided for the fee. Although one later letter from the administrator omitted the fee, this was judged poor communication rather than a waiver. The claim was dismissed, with each side bearing its own costs.

Key takeaways for consumers

1. Always read annexes and tariff schedules you sign alongside the main pension paperwork – early exit fees are often set out there, not just in the plan schedule.

2. Your signature on platform forms matters. Even if a trustee/administrator (RSA = Retirement Scheme Administrator) contracts with the platform on your behalf, a signed application and fee schedule can still bind you.

3. Watch out for phrases like "estimated amount" and "third-party charges may apply". They signal that separate platform fees may still be deducted at payout, even if not listed in a later letter.

4. Consider partial redemption if you need to cash out early; it may reduce or avoid penalties compared with a full encashment.

5. Act as soon as you become aware of a potential issue; time limits for complaints run from when you first had knowledge of the matter.

If you found this useful, check the full decision at this link https://shorturl.at/EW8MZ.

INSTAGRAM POSTS

On Instagram, we're refining how we share insights by breaking down decisions from the Arbiter for Financial Services into accessible summaries. These decisions often relate to familiar areas like banking, corporate services, and life and travel insurance.

From understanding the limits and responsibilities of a Basic Payments Account, to the importance of acting within legal timeframes when raising complaints about investments, these cases show how awareness and timely action can protect consumers.

Each post breaks down a real decision by the Arbiter for Financial Services and draws out practical lessons consumers can apply in their own financial lives.

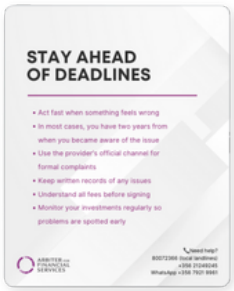
Featured on Instagram

Know your account

A recent case showed how a misunderstanding of a Basic Payments Account resulted in an unsuccessful complaint, reinforcing the importance of understanding account terms and keeping personal details up to date.

Timing matters

Another decision highlighted how a complaint was dismissed because it was filed outside the legal time limits, reminding consumers to act promptly and be aware of statutory deadlines when issues arise.



HAVE YOU BEEN THE VICTIM OF A SCAM?

As of 1 October 2025, the remit of the Arbiter for Financial Services has been widened to accept complaints from any person or entity that has fallen victim to a suspected fraudulent payment transaction involving financial services providers.

Therefore, any person (including individuals and companies of any size) who has fallen victim to a fraudulent payment transaction processed on or after 1 October 2025 through a financial services provider licensed in Malta can now lodge a complaint with the Arbiter for Financial Services for review.

Certain limitations may apply for transactions that occurred before this date. In any case, if you have been the victim of a scam, and you need further information, you can:

- call us on +356 21249245 or 80072366 during office hours; or
- send us a WhatsApp message on +35679249961; or
- send us an online enquiry (click here).

If you would you like to lodge a complaint, read further here.

ARBITER FOR FINANCIAL SERVICES

As we welcome 2026, we are proud to mark 10 years of the Office of the Arbiter for Financial Services. Over the past decade, the Office has worked to resolve disputes fairly and independently, strengthening consumer protection and trust in financial services. This milestone is an opportunity to reflect on the progress made, the cases resolved, and the continued commitment to clarity, accessibility and accountability in the financial sector.

The Office of the Arbiter for Financial Services is located in New Street in Regional Road, Msida MSD 1920. You can contact the Office of the Arbiter by calling 80072366 (local landlines only) or +356 21249245. Alternatively call or text on WhatsApp on +356 7921 9961.

Further information is available at www.financialarbiter.org.mt.