ARBITER FOR FINANCIAL SERVICES

NEWSLETTER

Issue 3 (December 2024)

Contents:

From 1 January 2025, the Office of the Arbiter for Financial Services (OAFS) will not charge a registration fee for new complaints. This reform aligns the OAFS with international best practices, as numerous jurisdictions already operate financial redress schemes without imposing charges on complainants.

This important change demonstrates the OAFS's commitment to enhancing access to justice through its redress mechanism by removing potential barriers for consumers from seeking resolution to their financial disputes.

For complaints registered up to 31 December 2024, the €25 registration fee will be refunded if the complainant withdraws the complaint or if both parties reach an agreement before the Arbiter issues a decision.

A WORD FROM THE ARBITER

Alfred Mifsud, Arbiter for Financial Services

Rising complaints and fraud concerns

Workload has continued to increase at the OAFS, with 233 complaints registered in the first 11 months of 2024, compared to 149 (excluding 75 complaints against one common service provider, which are frozen for regulatory reasons) that were registered in 2023. We consider this positively but with concern.

Positively because it indicates that consumers are becoming more aware of the services we offer; with concern because it is an indication that consumers have more to complain about.

In fact, we are seeing more complaints relating to fraud issues. Fraud includes one-shot unauthorised push payments (APP) complaints from bank customers, who pressed fraudulent links sent by fraudsters that were falsely personifying banks and payment institutions, as well as fraud relating to get-rich-quick schemes created by fraudsters to trap retail customers into crypto mania.

I am concerned not only with the quantity, but also with the quality of these fraud schemes. In some cases, we are going well beyond the usual €5,000 daily limit normally attached to accounts. We are seeing cases of high five figures and even six-digit losses.

There is the need for a co-ordinated national campaign to render consumers sensitive to the trickery and unbounded creativity of professional fraudsters, who are making an industry out of their deceit. I am co-ordinating with regulators and law enforcement authorities to launch such a campaign – the sooner the better.

However, we warn consumers to be more careful before parting with their savings. Get-rich-quick schemes are invariably too good to be true. They are carefully laid out to tempt vulnerable consumers to try their luck with a small sum. Once inside the scheme, it gets progressively more difficult to extricate themselves out, and they are quite often convinced to continue paying into the false scheme until, finally, the truth is exposed, with hurtful results – both financial and psycho-social.

Many complaints are being resolved using the model we published on how to allocate responsibility between the complainant and the bank. Early next year, we plan to issue Technical Notes on more sophisticated fraud schemes to guide service providers and customers on their respective roles and duties to protect and prevent this fraud.

Only two cases registered in 2023 are still awaiting adjudication. Most pending cases were registered in the second half of 2024. Generally, we are keeping within 90 days from date of final submissions to adjudication.

Hoping you had a lovely festive season and wishing everyone a happy New Year!

SELECTION OF CASE SUMMARIES

Our weekly LinkedIn posts typically feature a summary of a decision delivered by the Arbiter for Financial Services. Our aim is to inform stakeholders of disputes that are brought to our attention and the manner in which the Arbiter deals with these cases. In this section, we feature five posts providing a cross-section of decisions relating to the three main sectors: banking, life insurance and general insurance. All the Arbiter's decisions are online at financialarbiter.org.mt.

Unauthorised payments

The Arbiter received three separate complaints about unauthorised payments made from complainants' accounts with their financial services provider. In a typical case, the fraudster penetrated the communication channel normally used between provider and client, usually via SMS or e-mail.

Despite warnings not to click on links, the client clicked the link due to inattention. The fraudster then accessed the client's account and made a transfer, usually on a same-day basis to an overseas account. A dispute arose over who should bear the loss.

The financial services provider argued the fault was entirely the client's due to gross negligence in giving the fraudster access to their secret account credentials, facilitating the fraud. The provider claimed it had robust systems compliant with two-factor authentication requirements, so if the payment was fully authenticated by the client, the client must have been grossly negligent and fully responsible for the consequences of the fraud they suffered.

The Arbiter found that authentication of a payment does not automatically mean it was authorised by the client.

Payment service providers must prove gross negligence, not just ordinary negligence, by the client in making access credentials available to facilitate the specific payment, with the burden of proof on the provider.

Gross negligence depends on the circumstances of each case, lying somewhere between ordinary negligence and deliberate complicity. The Arbiter considered factors like the client's familiarity with online payments, if warnings were recently sent by the provider and if transaction monitoring systems should have flagged the payment as unusual.

To promote transparency and consistency in these cases, the Arbiter published a model allocating responsibility between the payment service provider and user, based on the circumstances. The model considers the strength of the provider's security systems, how recent the warnings to the client were and the client's level of participation in authorising the fraudulent payment beyond just disclosing credentials.

Applying the model to the specific cases, the Arbiter apportioned responsibility between the parties, ordering partial compensation to the clients – 20% in these cases since 80% of the responsibility was adjudicated to be that of the complainers. Each party was to bear their own costs.

Read the full decision on the three cases, ASF 011/2024, ASF 033/2024 and ASF 039/2024, which were not appealed, at these links: https://rb.gy/h18rwp, https://rb.gy/x3kzlp and https://rb.gy/jxazob.

Transferred funds

A complaint on the recovery of funds transferred to a corporate client of a financial services provider was not upheld by the Arbiter for Financial Services in a decision issued on 8 August 2024.

The complainant alleged that a corporate client of the financial services provider was involved in fraudulent activity with an online trading company that the complainant used for investments, which turned out to be a scam.

The complainant transferred €17,000 to the corporate client as instructed by the online trading company, believing it was for tax purposes, but later realised it was fraudulent. The complainant requested a refund of the amount transferred to the financial services provider's corporate client.

The financial services provider responded that they had no legal or contractual relationship with the complainant or the alleged scammers. They said they only provided payment reconciliation services to their corporate client and were not involved in the complainant's relationship with the trading company. The provider emphasised that they complied with all anti-money laundering and customer due diligence obligations for their corporate clients.

The Arbiter considered whether the complainant qualified as an "eligible customer" under the Arbiter for Financial Services Act. The Act defines an eligible customer as a consumer of a financial services provider, someone to whom the provider has offered a financial service or someone who has sought a financial service from the provider.

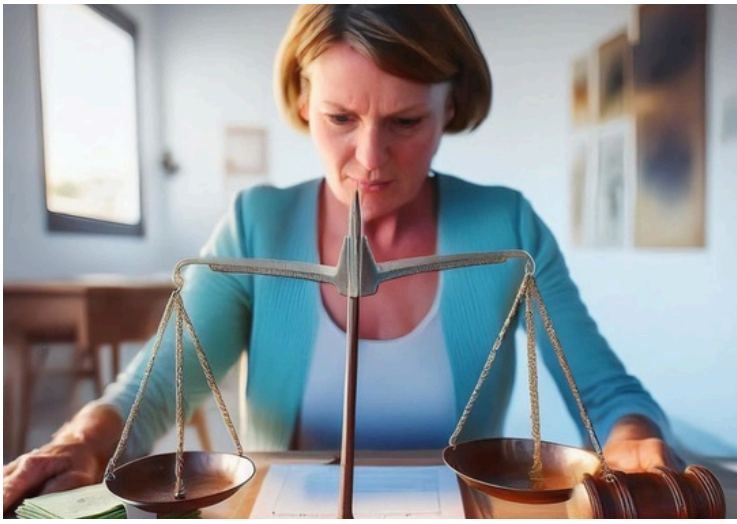
The Arbiter noted that the complainant had not contested the provider's claim that she was not their client. The complainant acknowledged not being a client of the financial services provider and only contacted them to try recovering funds transferred to the corporate customer's account.

The Arbiter found no evidence of a contractual relationship between the complainant and the financial services provider. Moreover, the complainant had not identified any specific shortcomings in the provider's conduct, but rather sought help to recover their funds.

The Arbiter determined that the complainant did not meet the definition of an "eligible customer" under the Act. Consequently, the Arbiter lacked the competence to deal with the merits of the complaint and dismissed it. However, the Arbiter made a non-binding recommendation that the financial services provider consider offering an *ex-gratia* payment to the complainant as a gesture of goodwill.

This recommendation, which was accepted, was based on the fact that the disputed payment occurred when the corporate client was already under the provider's Fraud Monitoring Programme, yet was allowed to continue operating for a 60-day grace period before account termination. The decision was not appealed. Both parties were to bear their costs.

Read the full decision on this case, ASF 112/2024, at this link: https://shorturl.at/qEi4g.



Life insurance payout on maturity

In a decision in August 2024, the Arbiter for Financial Services did not uphold a complaint against a life insurance company for additional payment beyond the amount declared at the policy's maturity. The complainant had based this request on the expectation of receiving a specified amount after having paid premium in a 20-year endowment life insurance policy.

The complainant alleged that the value of a life assurance policy at maturity was significantly less than the amount promised by the service provider's representative when the policy was sold. The complainant sought €23,000 from the provider, instead of the €16,053.85 offered at maturity, based on the expectation of receiving around €25,000 after investing €12,671.80 over 20 years.

The service provider refuted the allegation, stating that the maturity value could not be equivalent to the quotation's estimated maturity values since they were not guaranteed. The quotation presented three bonus rate scenarios, and the Important Notes explained that bonuses were not obligatory and depended on investment performance. The complainant was informed about potential rate changes and had a cooling-off period to cancel the policy.

The Arbiter examined the information given at the point of sale, the alleged promises made and how the product was sold. The quotation's three projected maturity values were based on different future bonus rates, indicating that these were estimates, not guarantees.

The complainant admitted that nothing was guaranteed in writing and that he had understood the quotation. The Arbiter noted the policy's overall performance, rendering around 3%, was not bad considering the circumstances, and the capital and declared gains were substantially guaranteed, apart from the life cover benefit.

The complainant provided no proof of having better alternatives or suffering opportunity loss due to choosing this policy based on the information provided.

The Arbiter concluded that the complaint was not fair and reasonable, and therefore was not upheld. Each party was to bear its own costs.

Read the full decision on this case, ASF 013/2024, which was not appealed, at this link: https://shorturl.at/N9nu7.

Medical expenses claim denied

A claim for compensate for medical expenses was turned down by the Arbiter for Financial Services in a decision in August following a breach in the policy conditions.

A customer filed a complaint against an insurance company on a rejected claim. The complainant had suffered a workplace injury in May 2021 and informed the insurance broker immediately after the incident occurred. He underwent surgery in May 2022, and attempted to claim compensation for medical expenses and recovery time. The insurance company denied the claim, citing late notification and lack of prior approval for the surgery.

The insurance provider defended its position by highlighting two key policy conditions that were breached: timely notification of the claim and obtaining pre-approval for expenses (except in emergencies).

They argued that the claim was reported 10 months after the incident, and the surgery was performed without their prior knowledge or approval. The insurer maintained that these breaches justified their rejection of the claim.

The Arbiter considered several factors in this case:

1. There was a significant delay in notifying the insurer about the claim. The incident occurred in May 2021, but the insurer was only informed in June 2022 – more than a year later.

2. The surgical intervention took place without the insurer's approval.

This potentially prejudiced the insurer's position since they were not given the opportunity to obtain a medical opinion from their experts, especially regarding the nine-week convalescence period that formed a substantial part of the claim.

3. No explanation was provided for the nine-month gap between the initial surgical consultation in August 2021 and the actual surgery in May 2022.

4. The complainant did not file a grievance against their insurance broker, who appeared to be the primary cause of the excessively late notification and the failure to obtain pre-approval for the surgery.

The Arbiter also noted that, while the complainant argued the insurer should be responsible for any faults attributable to the insurance broker, this was not the case. The broker's principal is the insured party, not the insurer.

Based on these considerations, the Arbiter decided that there was no valid reason to order the insurance provider to pay the claim, given the policy conditions that were breached by the complainant and/or their broker. The complaint was dismissed, and each party was ordered to bear its own costs.

Read the full decision on this case, ASF 059/2023, which was not appealed, at this link: https://shorturl.at/MjHgN.

Blocked payment accounts

Two complainants, an individual and a company under the same beneficial ownership, filed complaints against a service provider alleging that their accounts, holding approximately €72,000, were effectively blocked. The service provider had lost the ability to offer wire transfer services, and the complainants faced difficulties accessing their funds using the provider's card.

The individual complainant claimed this caused considerable stress since he needed the money to honour a property purchase agreement, forcing him to borrow from family.

The company complainant stated it was unable to settle its bills.

The service provider responded that, contrary to the complainants' statements, their accounts were active and funds accessible. Although SEPA payments were temporarily unavailable, the complainants could freely access funds via card transactions, ATM withdrawals and internal transfers between their accounts.

The provider admitted that account functionality was limited due to objective reasons but believed it had applied all possible measures to mitigate negative effects on the complainants.

The Arbiter determined that the service provider had indeed caused considerable stress and inconvenience, if not financial loss, through their inability to offer normal payment services. The alternatives offered were deemed inconvenient and unorthodox, falling well short of the expected service level from a licensed payment service provider.

However, the complainants did not present documentary evidence to support their claim for actual expenses (€700). The Arbiter noted that this was not an isolated failure but affected all the provider's customers. As such, the matter was referred to the Malta Financial Services Authority (MFSA) for guidance and direction under relevant regulatory provisions.

The Arbiter awarded €1,000 in moral damages to be shared between the personal complainant and company complainant in an 84:16 ratio, based on their respective blocked funds at the time of filing the complaint. Additionally, the service provider was ordered to refund all account service fees charged to both complainants from February 2024 to the date of the decision. The costs of the proceedings were to be borne by the service provider.

Read the full decision on these cases, ASF 128/2024 and ASF 129/2024, which were not appealed, at this link: https://shorturl.at/frDsd.

COURT OF APPEAL REVIEWS ARBITER'S DECISIONS

A recent Court of Appeal (Inferior Jurisdiction) judgement upheld the Arbiter's decision in a significant online fraud case and found no grounds to criticise the application of the model relating to allocation of responsibility between providers and users in case of payment fraud scams. On the other hand, the Court overturned a decision regarding account closure after previously undisclosed legal restrictions emerged.

In the first judgement, the Court found the bank's grievances unjustified, dismissing them and ordering the bank to pay compensation and legal costs.

The original complaint (ASF 116/2023) involved allegedly unauthorised transactions debiting €28,717 from the client's account, causing a €19,167 loss. This happened after the complainant, while abroad on 26 March 2023, received an SMS purportedly from the bank threatening to freeze the account unless security information was provided via a link.

The Arbiter ordered the bank to fully refund the €19,150 loss. Using the framework model to allocate responsibility, the Arbiter initially assigned a 90%/10% split between the bank and the complainant. However, considering the complainant's actions and the bank's delayed warnings, the Arbiter ultimately held the bank 100% liable.

The bank appealed, arguing the Arbiter misinterpreted facts, improperly assessed them and incorrectly applied the law.

It contended the complainant breached rules by not securing credentials, should have recognised the suspicious message and acted negligently. The bank claimed the Arbiter's model was prejudicial, abusive and *ultra vires*.

The Court found the Arbiter thoroughly examined the facts, consulted experts and developed a fair framework. It agreed banks were not doing enough to directly warn clients about spoofing/smishing risks.

The Court noted the Arbiter's observations that the bank's payment monitoring was defective, allowing a large transaction despite a previous reversal, and its high transaction limit contributed to the loss. Finding no arbitrary or unjust elements in the Arbiter's decision or model, the Court fully agreed with the Arbiter's well-founded considerations.

The second Court of Appeal judgment examined a complex situation involving bank account holders and their unsuccessful attempts to close their account and transfer funds. Two clients who opened an account in 2016 requested its closure in 2019, but received no response from the bank. They filed a complaint with the Arbiter for Financial Services in 2022 (ASF 097/2022).

The bank claimed legal impediments prevented them from complying with the closure request, though they initially couldn't disclose the specific reasons.

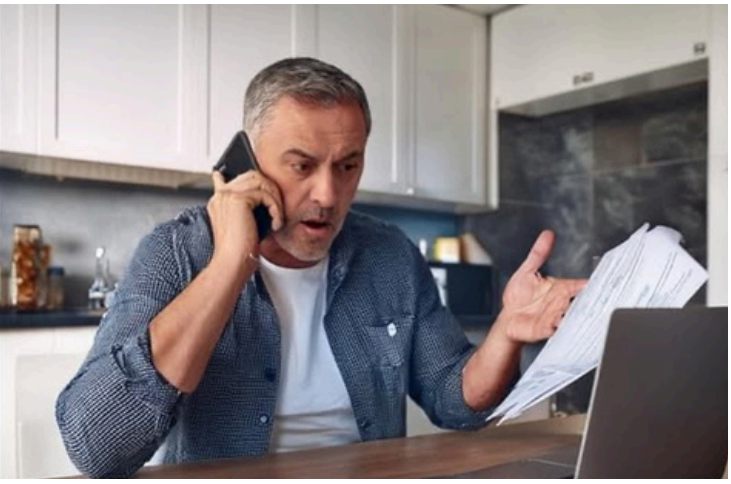
The Arbiter ruled in favour of the clients, ordering the account closure, fund transfer and 8% annual interest payment.

During the appeal proceedings, new evidence emerged: the bank had been served with a police garnishee order in October 2021 legally requiring them to block the accounts. The bank was prohibited from disclosing this information to either the clients or the Arbiter at the time.

The Court determined that the Arbiter's original decision was incorrect, though not due to any fault of the Arbiter who lacked crucial information when making the initial ruling. Now aware of the garnishee order, the clients could pursue action under Cap. 373 of Malta's Laws. The Court of Appeal reversed the Arbiter's decision and assigned all costs to the account holders, while the garnishee order remained in effect.

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. These are five typical posts related to fraudulent payments, a life policy and fake AI investment trading platforms. Apart from posting in English, we also post in Maltese.



On fraudulent payments

Important lessons from recent Arbiter for Financial Services decisions on fraudulent payments (cases ASF 011/2024, ASF 036/2024 and ASF 039/2024):

1. Be super cautious about clicking on links in SMSes or e-mails claiming to be from your bank, even if they look genuine. Banks don't send links this way!

2. Keep your login details and security credentials strictly confidential. Don't share them with anyone, even if they claim to be from your bank. Safeguard your login details and never share them with anyone, no matter how convincing they seem.

3. Be extra cautious when making unusual transactions, especially while travelling.

4. Always double-check payment details before confirming. If something seems off, contact your bank directly through official channels.

5. Report any suspicious activity to your bank immediately. Quick action can sometimes help recover funds.

6. Be wary of requests to "re-authenticate" or "validate" your account, especially if they come unexpectedly. Banks will never send you links asking you to validate your account or re-authenticate. Always double-check directly with your bank if unsure.

7. Stay informed about common scams. Pay attention to fraud warnings from your bank, especially direct communications. It's not enough to rely on your bank's general media warnings about scams.

8. Trust your instincts. If a transaction or request feels unusual, take a moment to verify before proceeding.

9. Familiarise yourself with your bank's security measures and proper online banking procedures.

10. Remember, your bank will never ask you to transfer money to a "safe account" or share your full PIN or password.

On life policies

Earlier this year, the Arbiter for Financial Services decided on the case (ASF 013/2024) relating to a 20-year life policy. Here are some key lessons for consumers:

1. When presented with quotes showing 'Projected Maturity Values' based on different future rates, remember they are estimates, not guarantees. Multiple scenarios indicate uncertainty!

2. Always read and understand the documentation provided, including any 'Important Notes'. Focus on what's officially documented rather than verbal promises. If you have questions, ask! The insurer should clearly explain the terms.

3. Long-term insurance products – such as a life policy or a retirement plan – typically have a 'cooling off' period after signing up (e.g., 30 days). You can cancel the policy if you change your mind during such a period. Know your rights!

4. Keep all correspondence related to your investment. A 2012 letter in this case showed revised (lower) estimates, highlighting how projections can change over time.

5. For long-term investments (like 20-year policies), understand that bonuses mentioned are usually not guaranteed. They depend on investment performance. Be aware that a lot can change. Initial projections may not reflect the final outcome.

6. Consider the overall return on your investment. In this case, a 3% return wasn't deemed unreasonable by the Arbiter, given the guarantees provided.

On fake AI investment platforms

SCAM ALERT: Beware of fake AI investment trading platforms!

A deepfake article is circulating on Facebook, claiming that a celebrity from Malta got rich using a particular AI investment trading platform. Don't fall for it! It's a SCAM designed to trick you into investing your hard-earned money.

The article uses fake screenshots, fabricated quotes and false promises of easy wealth to lure you in. Remember:

1. If it sounds too good to be true, it probably is!

2. There's no such thing as getting rich quick without effort or risk.

3. Always do your own research before investing your money.

Protect yourself from scammers:

NEVER share personal information or banking details with unknown parties.

NEVER disclose security authentication codes to anyone claiming to be from a trading platform.

IGNORE persistent calls from people pretending to act on behalf of an investment scheme.

NEVER allow remote access to your device through screen-sharing or remote desktop software since scammers may use this to steal your information or money.

INSTALL anti-phishing and anti-scam software on your devices since these can help block access to fraudulent trading platforms if you accidentally click on a link.

Stay vigilant and don't let scammers steal your hard-earned savings!

Spread the word to safeguard your friends and family from falling victim to this deepfake deception.

If you suspect you've been targeted by a scam, immediately contact your bank to stop any transactions and report it to the authorities. Acting quickly can help minimise potential losses.

Stay safe and informed out there!

On crypto asset investing

Here are some more lessons to be learned from recent decisions of the Arbiter for Financial Services involving crypto asset investing.

1. Be extra vigilant of scams and fraud in the crypto space. If an investment offer seems too good to be true, it probably is! Stay alert and sceptical, especially when dealing with unfamiliar parties or platforms.

2. Understand that crypto platforms primarily facilitate the transfer of funds and may not be involved in or responsible for investment decisions. So research and understand the investment before proceeding.

3. Verify transaction details before submitting instructions to your crypto service provider. You're responsible for ensuring accuracy!

4. Once you authorise a crypto transfer, it's final. Always double-check wallet addresses and transaction details before confirming.

5. Crypto providers aren't required to collect user data when you transfer to an external non-custodial wallet.

6. If you've been defrauded, notify local authorities. They can request any relevant information through proper legal channels.

7. The crypto market is high-risk and less regulated than traditional financial markets. Before investing, educate yourself on the risks and how to protect your assets.

On invoice scams

What should we look out for when we receive an invoice to ensure we are not being scammed?

1. Scammers often change account details on invoices or intercept emails to redirect payments to their accounts.

2. If you receive an invoice, even from a trusted source, and are pressured to pay quickly, it is crucial to verify the account details by calling trusted numbers and ensuring that payment recipients match the expected company or person.

3. A typical example of an invoice scam is a wedding booking, where scammers send a fake invoice with altered payment details, leading the victims to lose their life savings.

4. Other typical scams involve payment service providers and online retailers. So, it is important to be aware of the risks associated with clicking on fake invoices.

5. Be vigilant against requests for money or personal information, spelling errors in communications, and promises of easy rewards or harsh penalties.

6. Verify the legitimacy of invoices and take immediate action if fraud is suspected to maintain a secure online environment.

ARBITER FOR FINANCIAL SERVICES

TWO EDUCATIONAL VIDEOS ON SCAMS RELEASED

The OAFS has released two educational videos highlighting the growing sophistication of financial scams.

The first video, featuring an Einstein-like character to emphasise that anyone can fall victim to fraud, provides essential guidance on protecting oneself from scammers. It emphasises never sharing personal information or responding to unsolicited communications about banking details.

The second video introduces OAFS's new model for handling electronic messaging scams, which evaluates the responsibilities of both banks and consumers. This balanced approach, launched earlier this year, assesses each case individually to determine fair accountability.

The OAFS reminds consumers that banks will never request passwords or PINs via phone calls, nor threaten immediate service suspension through messages. If scammed, victims should contact their bank immediately. For those unsatisfied with their bank's response, the OAFS offers guidance through their complaint process at financialarbiter.org.mt.

Both videos, in Maltese and English, can be viewed on our website.

ARBITER FOR FINANCIAL SERVICES

GET IN TOUCH

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.

Don't miss out on valuable insights and updates!

Like our pages on Facebook, LinkedIn and Instagram to stay connected and receive our weekly posts every Friday!

On LinkedIn, we typically provide concise case summaries based on the latest decisions issued by the Arbiter.

On Facebook, we go beyond the decisions and share practical lessons from the Arbiter's deliberations. We also add tailored information to specific situations related to financial products and services arising from such decisions.

On Instagram, we provide quick, engaging insights from the Arbiter's decisions. We highlight key takeaways and practical tips.

Follow us