What’s new in economic crime and asset recovery

Anthony Wilson

What’s new in economic crime and asset recovery in the EU

- Money Laundering
- Cybercrime
- Asset Recovery

Money Laundering

US the main enforcer?

See https://thefinancialcrimenews.com/wp-content/uploads/2022/01/21st-Century-Bank-Fines-by-FCN-.pdf for an analysis of 95 fines of more than $10m since 2000 in the US

See https://sanctionscanner.com/blog/anti-money-laundering-aml-fines-of-2021-561 for a review of sanctions against banks 2021

See https://www.ft.com/content/7144ff53-5a17-477b-ab75-4f4a88b94fd2

NatWest fined £264.8 million for anti-money laundering failures see https://www.fca.org.uk/news/press-releases/natwest-fined-264.8million-anti-money-laundering-failures and for the sentencing remarks https://www.judiciary.uk/judgments/r-v-national-westminster-bank/ (2021)

FCA fines list 2022 fines | FCA

HMRC fines Businesses that have not complied with the regulations (2021 to 2022) - GOV.UK (www.gov.uk)

The next big mis selling scandal?

City lawyers are gearing up to make a wave of claims for mis sold crypto investments. The FCA have reminded consumers that there are very little consumer protections for those who buy non fungible tokens (NFTs) and crypto assets, and they are not eligible for protection with the FSCS.

FATF

- 25 Oct 2022
- The Financial Action Task Force is conducting a review of Recommendation 25 and its Interpretive Note (R.25/INR.25) on the transparency and beneficial ownership (BO) of legal arrangements. The FATF is also considering amendment of the definition of beneficial ownership in the glossary, to provide more clarity regarding legal arrangements
- At the March 2022 Plenary, the Financial Action Task Force (FATF) adopted amendments to Recommendation 24, and agreed to immediately start the work to update guidance on beneficial ownership, with a view to help support the implementation of the new requirements.

FATF –

- **Proposed Recommendation 25. Transparency and beneficial ownership of legal arrangements**

  - Countries should assess the risks of ~~take measures to prevent~~ the misuse of legal arrangements for money laundering or terrorist financing and take measures to prevent their misuse. In particular, countries should ensure that there is adequate, accurate and up-to-date ~~timely~~ information on express trusts and other similar legal arrangements, including information on the settlor(s), trustee(s) and beneficiary(ies), that can be obtained or accessed ~~in a timely fashion~~ efficiently and in a timely manner by competent authorities. Countries should consider ~~measures to~~ facilitateing access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

FATF

- **Recommendation 24. Transparency and beneficial ownership of legal persons**
  - Countries should assess the risks of ~~take measures to prevent the~~ misuse of legal persons for money laundering or terrorist financing, and take measures to prevent their misuse. Countries should ensure that there is adequate, accurate and ~~timely~~ up to date information on the beneficial ownership and control of legal persons that can be obtained or accessed rapidly and efficiently ~~in a timely fashion~~ by competent authorities, through either a register of beneficial ownership or an alternative mechanism. ~~In particular, c~~Countries ~~that have legal persons that are able to~~ should not permit legal persons to issue new bearer shares or bearer share warrants, and take measures to prevent the misuse of existing bearer shares and bearer share warrants. Countries~~, or which allow nominee shareholders or nominee directors,~~ should take effective measures to ensure that nominee shareholders and directors~~they~~ are not misused for money laundering or terrorist financing. Countries should ~~consider measures to~~ facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.
-

Egmont Group of 167 FIU's Strategic Plan 22-27

To leverage the core components of the EG's mission:

- To facilitate financial information and intelligence product exchanges between FIUs internationally
- To enable cooperation between FIUs to strengthen their capabilities and increase their overall effectiveness

The EG will focus on **Four Thematic Areas of Action with Strategic Goals** to fulfill its aspirations over the next five years:

1. **Enhance the framework for effective information exchange between FIUs**
2. **Strengthen cooperation with international partner organizations**
3. **Develop and promote knowledge of new or emerging AML/CFT methods and trends, best practices, and EG requirements**
4. **Enhance EG support for members and candidate FIUs**

Latest report FIU – FinTech Cooperation and Associated Cybercrime Typologies and Risks

https://egmontgroup.org/wp-content/uploads/2022/11/2022-Report-on-FIE-FinTech-Cooperation-and-Assoc.-Crimes.pdf

FATF Recommendation on New Technologies (15)

- The FATF Recommendation 15 (New Technologies) requires jurisdictions to address risks arising from new and emerging technologies and to strengthen anti-money laundering and counter-terrorism financing (AML/CFT) systems and controls.
- In addition, the FATF recently amended this recommendation to require jurisdictions to regulate virtual asset service providers (VASPs) for AML/CFT purposes. This includes ensuring such entities have effective systems and controls to monitor and ensure compliance with the AML/CFT measures contained within the FATF Recommendations

EU – see https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en

+ **Anti-Money Laundering and Terrorist Financing Directive V (AMLD V) - 2018/843/EU**

+ **Anti-Money Laundering and Terrorist Financing Directive IV (AMLD IV) - 2015/849/EU**

Documents

Supranational risk assessment report 2022
English (264.79 KB - HTML) Download

Annex to the 2022 supranational risk assessment report
English (1.92 MB - HTML) Download

Commission staff working document on the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing
English (768.52 KB - PDF) Download

EU – money laundering risk assessment

The new circumstances [the Covid Pandemic and aftermath] have enhanced the money laundering risk in many economic sectors and business activities. These risks include:

- misappropriation and fraud on funds granted as financial measures to protect national economies from the impact of the pandemic, or other public funds granted in the context of the pandemic
- taking over of businesses facing financial difficulties by ill-intentioned actors and criminal organisations
- increased opportunities for criminal groups to obtain revenues from selling unauthorised medical devices and illicit pharmaceuticals and vaccines, including to governments
- cybercrimes committed by taking advantage of the increasing volume of on-line purchases, including through the use of fraudulent identities; and
- corruption of civil servants when taking urgent measures, e.g. ordering specific medical supplies, and related simplification of procurement rules.

In order to ensure the effective implementation of EU asset freezing measures against persons and entities linked to the Russian aggression, the Commission set up the ‘Seize and Freeze’ Task Force. The aim of the Task Force is to coordinate actions taken by Union bodies and national authorities and to address any challenges in the implementation of EU sanctions. It identified of utmost importance to ensure swift progress in the negotiations of the Anti-Money Laundering package so as to ensure beneficial ownership information is available to competent authorities.

EU – money laundering risk assessment

According to a recent study carried out through the use of the DATACROS tool funded by the Internal Security Fund-Police, there are almost 31 000 firms in Europe (among which real estate, construction, hotels, and the financial and energy sector prevail) with Russian beneficial owners. 1 400 of them have ownership (up to 5%) held by 33 individuals subject to recent sanctions – the so-called oligarchs. In fact, a number of these firms already presented high-risk indicators before sanctions were issued: appearing in the Offshore Leaks database, unjustified corporate complexity, use of opaque legal arrangements or connections with high risk jurisdictions. This means that these firms could (and should) have raised alerts among competent and supervisory authorities before the recent events…

…The discussions in the framework of the 'Freeze and Seize' Task Force underline the difficulties in identifying the assets controlled by oligarchs as beneficial owners, often hidden behind complex legal structures across different jurisdictions. This is a major challenge for the enforcement of sanctions and for law enforcement investigative activities. Therefore, it is of outmost importance to ensure swift progress in the negotiations of the Anti-Money Laundering package so as to ensure beneficial ownership information is available to competent authorities.

This analysis is part of TOM – The Ownership Monitor, a joint-initiative by Transcrime and its spin-off Crime&tech: https://www.transcrime.it/en/stories/tom-the-ownership-monitor/

Mitigating Steps

Most legislative measures referred to in the two previous risk assessments have already been adopted, notably:

- the 5th Anti-Money Laundering Directive,
- the new Cash Controls Regulation ,
- the Directive on Countering Money Laundering by Criminal Law ,
- the Regulation on the introduction and the import of cultural goods
- the Directive on access to financial and other information ,
- the revision of the European Supervisory Authorities Regulations
- the adoption of Directive (EU) 2019/2177 , which amends the Solvency II Directive, the MiFID II Directive and the 4th Anti-Money Laundering Directive, and
- the adoption of the 5th Capital Requirements Directive , which removes the obstacles to cooperation between prudential and anti-money laundering/countering the financing of terrorism supervisors.

Mitigating Steps

On 20 July 2021, the Commission presented a package consisting of four legislative proposals to strengthen the EU AML/CFT provisions:

- A Regulation establishing a new EU AML/CFT Authority (“the AMLA Regulation”) ;
- A Regulation on AML/CFT, containing directly-applicable rules, including in the areas of Customer Due Diligence and Beneficial Ownership (“the AML/CFT Regulation”) ;
- A sixth Directive on AML/CFT (“AMLD6”), replacing the existing Directive 2015/849/EU (the fourth AMLD as amended by the fifth AMLD), containing provisions that will be transposed into national law, such as rules on national supervisors and FIUs in Member States ; and
- A revision of the 2015 Regulation on Transfers of Funds to trace transfers of crypto-assets (Regulation 2015/847/EU) (“the Transfers of Funds Regulation”) .

EU – new single rulebook

The proposed AML/CFT Regulation would constitute the central element of what is commonly referred to as an EU 'single rulebook' on AML/CFT.

It would replace the minimum rules of the EU AML Directives currently in force with detailed and directly applicable provisions.

The main issues addressed by the proposal include:

- the obligations imposed on entities required to prevent money laundering (‘obliged entities’);
- transparency of information regarding persons owning or controlling the customers of such entities;
- and the misuse of anonymous instrument (such as crypto-assets).

The Regulation would thus extend the list of obliged entities to include all crypto-asset service providers – as recommended by the Financial Action Task Force (FATF) – and streamline beneficial ownership requirements across the EU. It would also restrict transactions in cash, setting at EUR 10 000 a maximum cap for accepting or making payments in cash by persons trading in goods or providing services. Moreover, it would harmonise the EU approach to third countries with strategic deficiencies in their AML/CFT regimes.

EU – A new supervisory authority

The objective of the Authority shall be to protect the public interest, the stability of the Union's financial system and the good functioning of the internal market by:

- (a) preventing the use of the Union's financial system for the purposes of money laundering and terrorist financing;
- (b) contributing to identify and assess risks of money laundering and terrorist financing across the internal market, as well as risks and threats originating from outside the Union that are impacting, or have the potential to impact the internal market;
- (c) ensuring high-quality supervision in the area of anti-money laundering and countering the financing of terrorism ('AML/CFT') across the internal market;
- (d) contributing to supervisory convergence in the area of anti-money laundering and countering the financing of terrorism across the internal market;
- (e) contributing to the harmonisation of practices in the detection of cross-border suspicious flows of monies or activities by Financial Intelligence Units ('FIUs');
- (f) supporting and coordinating the exchange of information between FIUs and between FIUs and others competent authorities.

EUR-Lex - 52021PC0421 - EN - EUR-Lex (europa.eu)

EU – The AML Commission and Authority

The Commission proposed to task the AML/CFT Authority with direct supervisory powers. It should be operational in 2024. The Authority will start exercising its supervisory powers once the AMLD6 has been transposed and the new rules start to apply.

See The EU's AML Package: an examination – European Law Blog for a review of the Rule book

See also the proposed Regulation on Markets in Crypto-Assets resource.html (europa.eu)

EU – Regulation of Crypto-Assets

This Regulation lays down uniform rules for the following:

(a) transparency and disclosure requirements for the issuance and admission to trading of crypto-assets;

(b) the authorisation and supervision of crypto-asset service providers and issuers of asset-referenced tokens and issuers of electronic money tokens;

(c) the operation, organisation and governance of issuers of asset-referenced tokens, issuers of electronic money tokens and crypto-asset service providers;

(d) consumer protection rules for the issuance, trading, exchange and custody of cryptoassets;

(e) measures to prevent market abuse to ensure the integrity of crypto-asset markets.

Cybercrime – Danger to individuals and Infrastructure

- Two recent reports highlighted the extent to which fraud in the UK is now predominantly online fraud (see Progress combatting fraud (nao.org.uk) and (https://committees.parliament.uk/publications/31584/documents/177260/default/)
- NHS IT supplier held to ransom by hackers - BBC News
- Two days after a hacking group forced the nation's biggest gasoline pipeline to shut down, Commerce Secretary Gina Raimondo cautioned Sunday morning that cyberattacks against U.S. businesses and infrastructure are "here to stay" and becoming more frequent, joining a chorus of government officials urging Congress to help better prepare the private sector for future attacks. (see Cyberattacks Against U.S. Infrastructure Are 'Here To Stay' After 100-Gigabyte Colonial Pipeline Hack, Biden Official Warns (forbes.com))

EU Cybercrime pages see Cybercrime (europa.eu)

Cybercrime consists of criminal acts committed online by using electronic communications networks and information systems. The EU has implemented laws and supports operational cooperation through non-legislative actions and funding.

Cybercrime is a borderless issue that can be classified in three broad definitions:

- **crimes specific to the internet**, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts)
- **online fraud and forgery**: large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code
- **illegal online content**, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia

Many types of crime, including terrorism, trafficking in human beings, child sexual abuse and drugs trafficking, have moved online or are facilitated online. As a consequence, most criminal investigations have a digital component.

EU laws and actions aim to:

- improve the prevention, investigation and prosecution of cybercrime and child sexual exploitation
- build capacity in law enforcement and the judiciary
- work with industry to empower and protect citizens

EU Cybercrime Legislation

2020: Proposal for Interim Regulation on the processing of personal and other data for the purpose of combatting child sexual abuse

2019: Directive on non-cash payment
The directive updates the legal framework, removing obstacles to operational cooperation and enhancing prevention and victims' assistance, to make law enforcement action against fraud and counterfeiting of non-cash means of payment more effective.

2018: Proposals for Regulation and Directive facilitating cross-border access to electronic evidence for criminal investigations

2013: Directive on attacks against information systems

the directive aims to tackle large-scale cyber-attacks by requiring EU countries to strengthen national cyber-crime laws and introduce tougher criminal sanctions.

See also COE Convention on Cybercrime Full list - Treaty Office (coe.int)

EU – Cybercrime recent developments - Security

The Commission proposes a Regulation to establish common cybersecurity measures across the European Union institutions, bodies, offices and agencies. The key elements of the proposal for Cybersecurity Regulation:

- Strengthen the mandate of CERT-EU and provide the resources it needs to fulfil it;
- Require from all EU institutions, bodies, offices and agencies to:
  - Have a framework for governance, risk management and control in the area of cybersecurity;
  - Implement a baseline of cybersecurity measures addressing the identified risks;
  - Conduct regular maturity assessments;
  - Put in place a plan for improving their cybersecurity, approved by the entity's leadership;
  - Share incident-related information with CERT-EU without undue delay.
- Set up a new inter-institutional Cybersecurity Board to drive and monitor the implementation of the regulation and to steer CERT-EU;
- Rename CERT-EU from ‘Computer Emergency Response Team' to ‘Cybersecurity Centre', in line with developments in the Member States and globally, but keep the short name ‘CERT-EU' for name recognition.
- Proposal for Cybersecurity Regulation | European Commission (europa.eu)

EU – Asset Recovery and confiscation

In its strategy to combat organized crime (2021-2025) the Commission identified that recovery of criminal proceeds was hindered by:

- The narrow scope of EU confiscation legislation
- Asset Recovery Offices lack of powers to obtain interim freezing orders and to have access to public registers of data
- The lack of efficient management of recovered assets and their distribution to victims/society

And it proposed to revise the Confiscation Directive and the Council Decision on Asset Recovery Offices.

See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0170&qid=1632306192409

On 25 May 2022, the European Commission issued the Proposal for a Directive of the European Parliament and of the Council on asset recovery and confiscation (‘the Proposal’).

See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0245

1. This Directive shall apply to the following criminal offences:
(a) participation in a criminal organisation, as defined in Council Framework Decision 2008/841/JHA ;
(b) terrorism, as defined in Directive (EU) 2017/541 of the European Parliament and of the Council ;
(c) trafficking in human beings, as defined in Directive 2011/36/EU of the European Parliament and of the Council ;
(d) sexual exploitation of children and child pornography, as defined in Directive 2011/93/EU of the European Parliament and of the Council ;
(e) illicit trafficking in narcotic drugs and psychotropic substances, as defined in Council Framework Decision 2004/757/JHA ;
(f) corruption, as defined in the Convention drawn up on the basis of Article K.3(2)(c) of the Treaty on European Union on the fight against corruption involving officials of the European Communities or officials of the Member States of the European Union and in the Council Framework Decision 2003/568/JHA;

(g) money laundering, as defined in Directive (EU) 2018/1673 of the European Parliament and of the Council ;
(h) forgery of means of payment, as defined in Directive (EU) 2019/713 of the European Parliament and of the Council ;
(i) counterfeiting currency, including the euro, as defined in Directive 2014/62/EU of the European Parliament and of the Council ;
(j) computer-related crime, as defined in Directive 2013/40/EU of the European Parliament and of the Council ;
(k) illicit trafficking in weapons, munitions and explosives, as defined in the Protocol against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition, supplementing the United Nations Convention against transnational organized crime ;

(l) fraud, including fraud and other criminal offences affecting the Union's financial interests as defined in Directive (EU) 2017/1371 of the European Parliament and of the Council ;
(m) environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties as defined in in Directive 2008/99/EC of the European Parliament and of the Council , as well as offences related to ship pollution as defined in Directive 2005/35/EC as amended by Directive 2009/123/EC ;
(n) facilitation of unauthorised entry and residence, as defined in Council Framework Decision 2002/946/JHA , and Council Directive 2002/90/EC ;

EU – Asset Recovery & Confiscation

Scope – applies to offences

- Participation in a criminal organization, terrorism, trafficking in human beings, sexual exploitation of children and child pornography, illicit trafficking in narcotic drugs and corruption, as defined in the Convention drawn up on the basis of Article K.3(2)(c) of the Treaty on European Union.
- money laundering, forgery of means of payment, counterfeiting currency, including the euro,, computer-related crime, illicit trafficking in weapons, fraud, including fraud and other criminal offences affecting the Union's financial interest, environmental crime, including illicit trafficking in endangered specie and facilitation of unauthorised entry and residence, as defined in Council Framework Decision 2002/946/JHA, and Council Directive 2002/90/EC;
- Numerous offences committed whilst participating in a criminal organisation

BUT the provisions on tracing and identification of instrumentalities and proceeds, or property in Chapter II apply to all criminal offences as defined in national law which are punishable by deprivation of liberty or a detention order of at least one year.

EU – Asset Recovery & Confiscation

- *Article 4*
- **Asset tracing investigations**

- 1. To facilitate cross-border cooperation, Member States shall take measures to enable the swift tracing and identification of instrumentalities and proceeds, or property which may become or is the object of a freezing or confiscation order in the course of criminal proceedings.

EU – Asset Recovery & Confiscation

- **Asset recovery offices**

Each Member State shall set up at least one asset recovery office to facilitate cross-border cooperation in relation to asset tracing investigations

- (a) trace and identify instrumentalities, proceeds, or property whenever necessary to support other competent national authorities responsible for asset tracing investigations pursuant to Article 4;
- (b) trace and identify instrumentalities, proceeds, or property which may become or is the object of a freezing or confiscation order issued by another Member State;
- (c) cooperate and exchange information with other Member States' asset recovery offices in the tracing and identification of instrumentalities and proceeds, or property which may become or is the object of a freezing or confiscation order;
- (d) exchange information with other asset recovery offices in the Member States related to the effective implementation of Union restrictive measures where necessary to prevent, detect or investigate criminal offences.

Asset recovery offices shall be empowered to trace and identify property of persons and entities subject to EU targeted financial sanctions and for that purpose they shall cooperate with asset recovery offices and other relevant competent authorities in other Member States and exchange relevant information.

EU – Asset Recovery & Confiscation

- **Access to information**

Asset recovery offices are to have immediate and direct access to

(a) fiscal data, including data held by tax and revenue authorities;

(b) national real estate registers or electronic data retrieval systems and land and cadastral registers;

(c) national citizenship and population registers of natural persons;

(d) national motor vehicles, aircraft and watercraft registers;

(e) commercial databases, including business and company registers;

(f) national social security registers;

(g) relevant information which is held by authorities competent for preventing, detecting, investigating or prosecuting criminal offences.

EU – Asset Recovery & Confiscation

- **Conditions for access to information by asset recovery offices**

1. Access to information pursuant to Article 6 shall be performed only where necessary on a case-by-case basis by the staff specifically designated and authorised to access the information referred to in Article 6.

2. Member States shall ensure that staff of the asset recovery offices comply with the rules on confidentiality and professional secrecy as provided for under applicable national law. Member States shall also ensure that staff of asset recovery offices have the necessary specialised skills and abilities to perform their roles effectively.

3. Member States shall ensure that appropriate technical and organisational measures are in place to ensure the security of the data in order for asset recovery offices to access and search the information referred to in Article 6.

EU – Asset Recovery & Confiscation

- *Article 11* -**Freezing**

Member States shall take the necessary measures to enable the freezing of property necessary to ensure a possible confiscation of that property under Article 12.

- *Article 12*- **Confiscation**

Member States shall take the necessary measures to enable the confiscation, either wholly or in part, of instrumentalities and proceeds stemming from a criminal offence following a final conviction, which may also result from proceedings in absentia.

Member States shall take the necessary measures to enable the confiscation of property the value of which corresponds to instrumentalities or proceeds stemming from a criminal offence following a final conviction, which may also result from proceedings in absentia.

EU – Asset Recovery & Confiscation

Article 13

Confiscation from a third party

Article 14

Extended confiscation

EU – Asset Recovery & Confiscation

Article 15-**Non-conviction based confiscation**

1. Member States shall take the necessary measures to enable, under the conditions set out in paragraph 2, the confiscation of instrumentalities and proceeds, or property as referred to in Article 12, or which was transferred to third parties as referred to in Article 13, in cases where criminal proceedings have been initiated but the proceedings could not be continued because of the following circumstances:

(a) illness of the suspected or accused person;

(b) absconding of the suspected or accused person;

(c) death of the suspected or accused person;

(d) immunity from prosecution of the suspected or accused person, as provided for under national law;

(e) amnesty granted to the suspected or accused person, as provided for under national law;

(f) the time limits prescribed by national law have expired, where such limits are not sufficiently long to allow for the effective investigation and prosecution of the relevant criminal offences.

3. Before a confiscation order is issued by the court, Member States shall ensure that the affected person's rights of defence are respected including by awarding access to the file and the right to be heard on issues of law and fact.

EU – Asset Recovery & Confiscation

Article 16

Confiscation of unexplained wealth linked to criminal activities

1. Member States shall take the necessary measures to enable the confiscation of property, where confiscation is not possible pursuant to Articles 12 to 15 and the following conditions are fulfilled:

(a) the property is frozen in the context of an investigation into criminal offences committed in the framework of a criminal organisation;

(b) the criminal offence pursuant to point (a) is liable to give rise, directly or indirectly, to substantial economic benefit;

(c) the national court is satisfied that the frozen property is derived from criminal offences committed in the framework of a criminal organisation.

2. When determining whether the frozen property is derived from criminal offences, account shall be taken of all the circumstances of the case, including the specific facts and available evidence, such as that the value of the property is substantially disproportionate to the lawful income of the owner of the property.

EU – Asset Recovery & Confiscation

Chapter V – Safeguards includes

Article 23

Legal remedies

1. Member States shall ensure that the persons affected by the measures provided for under this Directive have the right to defence, to an effective remedy, and to a fair trial in order to uphold their rights.

2. Member States shall provide for the effective possibility for the person whose property is affected to challenge the freezing order pursuant to article 11 before a court, in accordance with procedures provided for in national law. Where the freezing order has been taken by a competent authority other than a judicial authority, national law shall provide that such an order is first to be submitted for validation or review to a judicial authority before it can be challenged before a court.