

Recent Developments in EU Anti-Money Laundering

Some Critical Observations

Jean-Baptiste Maillart, Benjamin Vogel



eucrim

European Law Forum: Prevention • Investigation • Prosecution

Article

ABSTRACT

The article critiques recent EU AML moves—4AMLD and the Commission's 2016 package—through five lenses: scope, ECDD, beneficial ownership, FIUs, and criminalisation. It welcomes extending coverage to gambling and lowering the cash threshold, but flags gaps (e.g., construction/property developers; ambiguity on letting agents) and says virtual-asset gatekeepers belong inside the regime (as the 2016 proposal suggests). The Commission's mandatory enhanced CDD list for high-risk third-country dealings may curb forum-shopping but risks cost, de-risking, and lost intelligence; a smarter calibration of the risk-based approach is urged. Beneficial ownership registers are innovative yet fragile without verification and clear sanctions, and wider/public access raises unresolved data-protection questions. Expanding FIU powers (direct access to obliged-entity data; bank-account registries) could speed analysis but needs tighter legal limits to avoid incoherence and privacy problems. On criminalisation, the piece cautions against over-broad predicate catalogues and negligence-based offences; it argues for careful treatment of self-laundering and prioritising robust enforcement of preventive duties over stretching criminal law.

AUTHORS

Jean-Baptiste Maillart

Researcher, Ph.D. Candidate at the University of Geneva
Max Planck Institute for Foreign and International Criminal Law, Freiburg i.Br.

Benjamin Vogel

Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law (formerly Max Planck Institute for Foreign and International Criminal Law)

CITATION SUGGESTION

J. Maillart, B. Vogel, "Recent Developments in EU Anti-Money Laundering", 2016, Vol. 11(4), eucrim, pp179–183.
DOI: <https://doi.org/10.30709/eucrim-2016-022>

Published in

2016, Vol. 11(4) eucrim pp 179 – 183

ISSN: 1862-6947

<https://eucrim.eu>



Since the adoption of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances in 1988,¹ many efforts have been made to strengthen the anti-money laundering (AML) regime at the international level and also within the European Union, where several directives to this effect have been adopted since 1991.² The fourth and latest EU Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorism financing (4AMLD) was adopted by the European Parliament and the Council in May 2015 in order to reinforce the efficacy of the European Union's action in this area,³ thereby to a large extent following the Recommendations of the Financial Action Task Force (FATF), which had been revised in 2012.⁴ In response to recent terrorist attacks across Europe, the European Commission then published an action plan in February 2016 to "further step up the fight against the financing of terrorism."⁵ This action plan sets out a series of measures pertaining directly to money laundering and terrorism financing, which eventually led to the publication (on 5 July 2016) of a Proposal for a Directive amending Directive 2015/849⁶ and furthermore to the Roadmap of 25 October 2016 aiming at harmonising the criminalisation of money laundering.⁷ This article will assess some of the most innovative measures adopted in the 4AMLD or proposed in 2016 by the European Commission. It will address the enlargement of the scope of the anti-money laundering/counter-terrorism financing (AML/CTF) regime, the proposed rules for high-risk third countries, the creation of national beneficial ownership registries, the proposed enhancement of the powers of Financial Intelligence Units (FIUs), and finally the envisaged harmonisation of the criminal offence of money laundering. Although some measures can be welcomed, others must be subjected to a more nuanced appraisal.

I. Scope of the AML Regime

The 4AMLD further strengthened the European AML framework. Notably, the scope of obliged entities has been extended to sectors that are particularly vulnerable to money laundering. The Directive rightly⁸ addressed the risks relating to gambling services by extending its applicability to all providers of such services⁹ and not only to casinos as provided for by the 2005 third Anti-Money Laundering Directive (3AMLD).¹⁰ Moreover, the threshold for cash transactions above which persons trading in goods qualify as obliged entities has been reduced from €15,000 EUR to €10,000.¹¹

However, the 4AMLD still contains important *lacunae* with respect to the scope of obliged entities. Some economic activities with high money laundering potential have indeed not yet been included in the EU AML framework. In particular, virtual currency exchange platforms (e.g., Bitcoin, Litecoin, Liberty Reserve)¹² and custodial wallet providers are not covered by the 4AMLD.¹³ Yet, as the European Commission points out, "[t]ransactions with virtual currencies benefit from a higher degree of anonymity than classical financial fund transfers"¹⁴ and therefore entail a money laundering risk, especially with respect to the concealment phase.¹⁵ This risk is amplified by the "opaque and technologically complex nature of the industry, and the lack of regulatory safeguards."¹⁶ Hence, the Commission proposes designating "all gatekeepers that control access to virtual currencies, in particular exchange platforms and wallet providers"¹⁷ as obliged entities under the 4AMLD, therefore subjecting them to appropriate customer due diligence obligations (CDD) and reporting obligations.¹⁸ Such an extension of the scope of obliged entities constitutes a potentially¹⁹ important improvement. In contrast, it seems unsatisfactory that neither the 4AMLD nor the current proposal addresses the presumably high money laundering risk in the construction sector, especially with regard to property developers.²⁰ Furthermore, the 4AMLD remains somewhat ambiguous on whether letting agents are considered obliged entities.²¹ Finally, the Commission proposes new rules for payment cards, which are rather questionable in terms of their effectiveness, by lowering the threshold from 250 EUR to 150 EUR for non-reloadable pre-paid instruments to which customer due diligence measures apply. It is indeed hard to

see how this rather modest reduction of the threshold amount could significantly affect the use of such cards for money laundering or terrorism financing.

II. Enhanced Customer Due Diligence Obligations

The 4AMLD provides for enhanced customer due diligence (ECDD) for cases that represent a higher risk of money laundering or terrorism financing. However, with the exception of cross-border correspondent relationships of credit institutions with a third-country,²² and transactions or business relationships with politically exposed persons (PEPs),²³ the Directive does not specify which ECDD measures the obliged entities are required to undertake in order to adequately respond to the qualified risk. With regard to dealing with entities in high-risk third countries, the Commission now fears that the lack of harmonisation of such measures could lead to forum-shopping, depending on the stringency of individual Member States' legal frameworks.²⁴ In its 2016 proposal, it therefore proposes the insertion of a cumulative list of ECDD that obliged entities would need to apply to transactions with high-risk third countries.²⁵

While concerns regarding deficient harmonisation and forum-shopping are pertinent, it should be noted that their relevance is not confined to ECDD with respect to high-risk third countries. Similar concerns could also be directed at standard AML CDD. The 2012 FATF Recommendations and the 4AMLD have reinforced the "risk-based" approach to CDD, thereby avoiding ineffective rigidity (the so-called "tick-the-box approach"). However, the risk-based approach does effectively allow for considerable flexibility on the part of national legislators and obliged entities in the imposition and application of AML/CTF measures.²⁶ Such flexibility not only creates problems with regard to the effective harmonisation of AML measures. Too much leeway in obliged entities' risk assessment is also problematic with regard to the rights of customers, as it can undermine their contractual rights vis-à-vis the obliged entity. By citing their individual risk policy, obliged entities will often be provided with a relatively easy way out of their contractual obligations, even in the absence of an objectively substantiated AML/CTF risk. This gives rise not least to the risk of illegitimate discriminatory business practices. One might therefore argue that the Commission's attempt to provide clearer rules for ECDD signals a more general need to recalibrate and further specify the risk-based approach to CDD. In this respect, however, the 2016 proposal also suggests that overly strong reliance on a CDD "rules-based" approach will not necessarily enhance the effectiveness of AML efforts. The proposed provision is very burdensome and cost-intensive and might therefore invite frequent "de-risking" by obliged entities, potentially pushing business with high-risk third countries into the hands of less regulated or illicit operators and thereby making the competent authorities lose access to valuable financial intelligence. While the Commission's proposal repeats the entirety of the FATF Recommendation's ECDD measures,²⁷ one should note that, according to the FATF, its list of measures constitutes "*examples* of enhanced CDD measures that could be applied for higher risk business relationships,"²⁸ while, for high-risk third country transactions, the Commission proposal now states that obliged entities "*shall apply at least all* the [FATF] enhanced customer due diligence measures" (emphasis added).²⁹ Although such a wholesale adoption of the FATF ECDD measures might be justified in view of the special risk posed by high-risk third countries, in other constellations of ECDD, a blanket reference to the FATF's list would hardly ensure reasonable risk management. One can only hope that future action by the European legislator and guidelines by European Supervisory Authorities will lead to greater refinement of ECDD measures.

III. Beneficial Ownership of Legal Entities and Trusts

In line with the FATF Recommendations,³⁰ the 4AMLD obliges Member States to "ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership,"³¹ and to "ensure that this information is held in a central

registry in each Member State.”³² Similar obligations are required for the trustees of any express trust governed under the law of a Member State.³³ By ensuring the transparency of financial flows involving legal entities and trusts, such beneficial ownership registries (BORs) are arguably the most innovative element of the 4AMLD, but also one of its most controversial elements. The current framework raises questions, particularly with regard to its effectiveness and the adequate protection of personal data.

First, regarding the framework’s effectiveness, it is important to note that neither the 4AMLD nor the Commission’s new proposal specifies a mechanism that would ensure the accuracy of BORs’ content. This is worrisome, as legal entities involved in money laundering or terrorism financing are likely to actively conceal their backers. Without an effective verification mechanism, BORs will likely lead to serious infringements of the data protection rights of legitimate economic actors without delivering a tangible benefit over illegitimate ones. Incidentally, the Directive does not oblige Member States to provide for sanctions in the event that legal entities or trustees provide the authorities with inaccurate beneficial ownership information. Second, the Commission’s proposal amplifies data protection issues regarding access to BORs. Besides access by competent authorities, FIUs, and obliged entities for the purpose of CDD, the 4AMLD grants BORs access to any person that can demonstrate a “legitimate interest” in obtaining the beneficial ownership information of corporate and other legal entities. In this respect, the Commission now intends to go a significant step further. It proposes an amendment to Directive 2009/101/EC³⁴ requiring corporate and other legal entities as well as such trusts that are conducting a business³⁵ to disclose certain beneficial ownership information, thereby allowing for the identification of the beneficial owners as well as the nature and extent of the beneficial interest held. This information would be publicly available, in this way forgoing the hitherto existing “legitimate interest” access requirement.³⁶ The proposed amendment to Directive 2009/101/EC explains that such publication of beneficial ownership information is meant to enable third parties and civil society at large to contribute to the preventive efforts through enhanced public scrutiny. While the proposal’s objective is laudable, one must question whether data protection implications have been sufficiently addressed. The 4AMLD³⁷ and the proposed amendment to Directive 2009/101/EC³⁸ both acknowledge the potential for abuse of beneficial ownership information – explicitly mentioning the dangers of fraud, kidnapping, blackmail, violence or intimidation – and therefore allow for exemptions from making this information public on a case-by-case basis in exceptional circumstances. To ensure effective and proportionate harmonisation throughout the Union, one wishes that the European legislator would specify what these circumstances are. Furthermore, the 4AMLD implies that access by obliged entities to BORs can be limited (as only competent authorities and FIUs are granted access “without any restriction”),³⁹ thereby avoiding an excessive dissemination of details of a beneficial interest. Here too, clarification regarding the extent of possible restriction to access would allow for a more coherent harmonisation and thereby a strengthening of BORs.

IV. Enhanced Powers of FIUs

The European Commission’s 2016 proposal also aims at enhancing the powers of FIUs in two respects. First, it proposes to significantly expand the data-gathering powers of FIUs, authorising them to request data “from any obliged entity information [...] even if such obliged entity did not file a prior [suspicious transaction] report”.⁴⁰ Under the 4AMLD, access by FIUs to information held by obliged entities is indeed limited, as FIUs are only authorised to obtain “additional information.”⁴¹ Consequently, as the Commission points out, “[t]hat information is currently limited in certain Member States by the requirement [of] a prior suspicious transaction report.”⁴² This new power would certainly help FIUs to improve their analytical capacity. Insofar as the Commission refers to “the latest international standards”⁴³ to justify this reform, however, it must be noted that the current FATF Recommendations still refer to FIUs’ power to obtain “*additional* information from reporting entities” (emphasis added).⁴⁴ With regard to other “commercially held data,” the FATF requires FIU access to this data only “where appropriate.”⁴⁵ Given that the Commission’s 2016 proposal entails the

potential to transform FIUs into investigative bodies in their own right, it seems crucial to further specify the FIUs' new investigative competence, in particular by clarifying when a request for information is appropriate. Otherwise, the new power will not only cause serious data protection problems, but likely lead to great incoherence in the way in which different Member States define its scope.

Second, the Commission's proposal envisages the creation of an automated central mechanism – such as a central registry or an electronic data retrieval system – at the Member State level, allowing for the swift identification of bank and payment account holders by the competent authorities, including FIUs. Up until now, the 4AMLD had only “recommended” such an instrument, but refrained from making it mandatory.⁴⁶ As the Commission rightly states, the new mechanism would undoubtedly “lead to a faster detection – both nationally and internationally – of suspicious ML/TF transactions, and improve preventive action.”⁴⁷ However, although the content of the envisaged central mechanism is currently very limited (including the customer-account holder and IBAN number), the Commission appears to anticipate that some Member States might go beyond this minimum and feed the mechanisms with other information they consider necessary for the prevention of money laundering and terrorism financing. Given that the proposal requires Member States to ensure that FIUs are able to provide information contained in the mechanism to any other FIU – i.e., to ensure a cross-border exchange of the information – one should caution against too broad a content of the mechanism. This might otherwise create data protection problems in other Member States and thereby complicate cross-border cooperation.⁴⁸

V. Criminalisation of Money Laundering

On 25 October 2016, the European Commission published a roadmap on a proposal for a Directive on the Criminalisation of Money Laundering, which would be the very first directive of its kind, since the European Union has so far focused only on preventive measures in this respect. The aim of the proposal is to “introduce minimum rules regarding the criminal offence of money laundering and to approximate sanctions”.⁴⁹ According to the Commission, “[t]he current criminal framework against money laundering across Europe is neither comprehensive nor sufficiently coherent to be fully effective, with the consequence of enforcement gaps and obstacles to information exchange and cooperation between the competent authorities in different countries.”⁵⁰ The Commission assumes that “the current situation does not ensure effective enforcement or adequate deterrence,” and that an “often low level of sanctions” and “low prosecution rates” contribute to a risk of “forum shopping” in that criminals are “carrying out financial transactions where they perceive anti-money laundering measures to be weakest.”⁵¹

So far, it is not yet clear what exact shape harmonisation would take. It will be important to see how the Commission addresses a number of issues, as the offence of money laundering does indeed raise a number of difficult questions that can even pose challenges for some Member States' constitutional law. To begin with, one could contemplate whether or to what extent self-laundering (i.e., laundering of the proceeds of one's own criminal activity) is covered. Not least due to the privilege against self-incrimination, some legal orders find it difficult to extend the offence's scope accordingly. In order to address such concerns, any harmonisation at least requires a sufficiently delimited statutory definition of self-laundering.⁵² Furthermore, drafters of the Directive need to thoroughly think about the adequate scope of predicate offences (i.e., those offences resulting in generation of the criminal proceeds). While the FATF recommends that “[c]ountries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences,”⁵³ the European legislator will have to address both proportionality concerns and unwanted practical consequences of an overly broad catalogue of predicate offences. Given that the offence of money laundering serves as the bedrock of and overreaching reference point for the preventive anti-money laundering framework (especially CDD), the drafters must take into account the resulting knock-on

effects on obliged entities, in particular the overburdening effect and resulting phenomenon of “de-risking.”⁵⁴ The purported current ineffectiveness of criminal law enforcement should thus only be one of several important considerations. Finally, as regards the *mens rea* element, the Commission may be tempted to go beyond the intent requirement (as included in the 1988 Vienna Convention⁵⁵ and the 2000 United Nations Convention against Transnational Organized Crime),⁵⁶ and also criminalise the negligent commission of money laundering, as optionally provided for by the 2005 Council of Europe Convention.⁵⁷ While an offence of negligence might alleviate the prosecutor’s evidential burden, it is not entirely clear whether this would improve the effectiveness of anti-money laundering. Negligence would not only often be treated as relatively little blame-worthy, consuming scarce resources of prosecuting agencies without ultimately leading to the imposition of deterrent sanctions. One also needs to question the impact that the threat of criminal punishment might have on obliged entities’ willingness to cooperate extensively with the authorities in the fight against money laundering, given that simple mistakes in compliance practice might make them criminally liable. If the legislator is seeking to enhance public-private partnerships in AML/CTF, a broad threat of punishment might not offer the most constructive framework for dialogue. Consequently, instead of criminalizing the negligent handling of proceeds of crime, it would better to focus legislative attention and enforcement practice on breaches of obliged entities’ preventive duties, especially their reporting requirements. Priority should thus be given to an effective implementation of the 4AMLD’s existing sanctions provisions.⁵⁸

1. United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 20 December 1988.↵
2. The first one was Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.↵
3. See the Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and the Proposal for a regulation on information accompanying transfers of funds to secure “due traceability” of these transfers, both adopted by the European Commission on 5 February 2013.↵
4. FATF (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, updated October 2016.↵
5. Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing, COM/2016/050 final, 2 February 2016.↵
6. Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, COM/2016/450 final, 5 July 2016.↵
7. Proposal for a Directive on criminalisation of money laundering, Roadmap, 25 October 2016.↵
8. See, e.g., 4AMLD, recital 21: “The use of gambling sector services to launder the proceeds of criminal activity is of concern”.↵
9. 4AMLD, article 2(1)(3)(f). However, according to article 2(2), Member States can remove these providers – with the exception of casinos – partially or completely from the list of obliged entities if a low money laundering risk is evidenced.↵
10. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, article 2(1)(3)(f).↵
11. 4AMLD, article 2(1)(3)(e). For comparison, see 3AMLD, article 2(1)(3)(e).↵
12. 637 crypto-currencies exist at the moment (www.coinmarketcap.com, last accessed on 7 December 2016).↵
13. On the vulnerability of virtual currency exchange platforms and custodial wallet providers to money laundering, see, e.g., FATF (2014), *Virtual Currencies: Key Definitions and Potential AML/CTF Risks*.↵
14. *Supra* note 6, p. 12.↵
15. Money laundering is traditionally understood as a threefold process: 1) Concealment of the criminal proceeds in the financial system; 2) Conversion of the criminal proceeds, the purpose of which is to further conceal the origin and ownership of the initial criminal money by transferring it several times; 3) Integration into the formal or legal economy. See, e.g., R. Booth, S. Farrell, G. Bastable & N. Yeo, *Money Laundering: Law and Regulation*, Oxford, 2011, pp. 3-4; R. Durieu, *Rethinking Money Laundering and Financing of Terrorism in International Law: Towards a New Global Legal Order*, Leiden, Boston, 2013, pp. 240-262.↵
16. *Supra* note 6, p. 12.↵
17. *Ibid.*, p. 7.↵
18. The Commission proposes to extend article 2(1)(3) 4AMLD to cover “(g) providers engaged primarily and professionally in exchange services between virtual currencies and fiat currencies” and “(h) wallet providers offering custodial services of credentials necessary to access virtual currencies”. For legal certainty reasons, a definition of “virtual currency” is also proposed in article 3(c)(18): “(18) ‘virtual currencies’ means a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically”.↵
19. One must note, that, for the time being, the relevance of virtual currencies for money laundering or terrorism financing remains limited. However, this situation is likely to change once virtual currencies are more increasingly used in the legitimate economy. See, e.g., HM Treasury/Home Office, *UK national risk assessment of money laundering and terrorism financing*, London, October 2015, p. 79.↵

20. Cf. K. Bussmann, *Dark figure study on the prevalence of money laundering in Germany and the risks of money laundering in individual economic sectors*, Summary, Halle, August 2015, p. 9.↵
21. Whilst article 2(1)(3)(d) 4AMLD only mentions “estate agents”, it is conceivable that this includes letting agents as mentioned in recital 8. However, a recent draft resolution by Members of the European Parliament recommends amending article 2(1)(3)(d) to explicitly include “letting agents” (see draft European Parliament legislative resolution on the proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849, 7 November 2016).↵
22. 4AMLD, article 19.↵
23. 4AMLD, article 20. It is worth pointing out that the 4AMLD has extended the requirement to apply ECDD with respect to domestic PEPs and PEPs of international organisations. The 3AMLD had envisaged this requirement only with respect to foreign PEPs, i.e., PEPs who reside in another Member State or in a third country (see 3AMLD, article 13).↵
24. *Supra* note 6, p. 15.↵
25. *Ibid.*, pp. 31-32. Note that article 18(4) of the 4AMLD already provides that the European Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Markets Authority (“ESAs”) shall issue guidelines addressed to competent authorities and to credit institutions and financial institutions on the risk factors to be taken into consideration and the measures to be taken in situations where ECDD are appropriate. However, it appears that such guidelines are judged as insufficient in ensuring comprehensive harmonisation of ECDD throughout the Union.↵
26. See 4AMLD, article 13(2).↵
27. Cf. FATF Recommendations 2012, p. 67.↵
28. *Ibid.*↵
29. *Supra* note 6, p. 31.↵
30. *Supra* note 4.↵
31. 4AMLD, article 30(1).↵
32. 4AMLD, article 30(3).↵
33. 4AMLD, article 31(1) and (4). Note that article 31(4) only applies to trusts that generate tax consequences.↵
34. Directive 2009/101/EC of the European Parliament and the Council of 16 September 2009 on the coordination of safeguards for the protection of the interests of members and third parties, which Member States require of companies within the meaning of the second paragraph of article 48 of the Treaty, with a view to making such safeguards equivalent.↵
35. *Supra* note 6, p. 39.↵
36. *Ibid.*, p. 40.↵
37. 4AMLD, article 30(9).↵
38. *Supra* note 6, p. 40.↵
39. 4AMLD, article 30(5).↵
40. *Supra* note 6, p. 35.↵
41. 4AMLD, article 32(3).↵
42. *Supra* note 6, p. 14.↵
43. *Ibid.*, p. 13.↵
44. *Supra* note 4, p. 98↵
45. *Ibid.*↵
46. 4AMLD, recital 57.↵
47. *Supra* note 6, p. 14.↵
48. The Commission merely provides that “such registries should store the minimum data necessary to the performance of AML/CFT investigations, the concerned data subjects should be informed that their data are recorded and accessible by FIUs and are given a contact point for exercising their rights of access and rectification” (*supra* note 6, p. 15).↵
49. *Supra* note 7.↵
50. *Ibid.*↵
51. *Ibid.*↵
52. For an example of such delimitation, cf. the new Section 261 para. 9 of the German Penal Code: according to this provision, any party to the commission of the predicate offence is punishable for money laundering only when he distributes the proceeds to others and, in doing so, conceals their unlawful origin.↵
53. *Supra* note 4, see Recommendation 1.↵
54. See *supra*.↵
55. *Supra* note 1, article 3(2).↵
56. United Nations Convention against Transnational Organized Crime, 15 November 2000, article 6(1).↵
57. Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 16 May 2005, article 9(3). See also Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, 8 November 1990, article 6(3)(a).↵
58. 4AMLD, articles 56-62.↵

access article published under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) licence. This permits users to share (copy and redistribute) the material in any medium or format for any purpose, even commercially, provided that appropriate credit is given, a link to the license is provided, and changes are indicated. If users remix, transform, or build upon the material, they may not distribute the modified material. For details, see <https://creativecommons.org/licenses/by-nd/4.0/>.

Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and “criministrative” law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU’s financial interests – a key driver of European integration in “criministrative” justice policy.

Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.

All content is freely accessible at <https://eucrim.eu>, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.

The project is co-financed by the [Union Anti-Fraud Programme \(UAFP\)](#), managed by the [European Anti-Fraud Office \(OLAF\)](#).



**Co-funded by
the European Union**