Impact of Organised Crime on the EU’s Financial Interests

Policy Department for Budgetary Affairs
Authors: Jack MALAN, Ivan BOSCH CHEN et al. (CSES)
Directorate-General for Internal Policies
PE 697.019– July 2021
Impact of Organised Crime on the EU’s Financial Interests

Abstract
This analytical study, requested by the European Parliament’s Committee on Budgetary Control, examines the impact of organised crime on EU’s finances. Taking together the expenditure and revenue sides, the research suggests that between 1% and 2% of the EU budget is defrauded each year. The study also assesses measures at the EU and Member State levels to combat the problem, and recommends actions to help reinforce these measures.
This document was requested by the European Parliament's Committee on Budgetary Control. It designated Ms Caterina CHINNICI MEP to follow the study.

AUTHORS
The principal authors of this study were Jack MALAN and Ivan BOSCH CHEN from the Centre for Strategy & Evaluation Services (CSES).

The CSES research team was composed of: Michaela BRADY, Clara BURILLO, Marta DIMAURO, James EAGER, Marta GUASP TESCHENDORFF, Elias NACER, and Dr Dorottya SALLAI. Section 4 was produced by Dr Mihály FAZEKAS (Scientific Director, Government Transparency Institute and Assistant Professor, Central European University) and Olena NIKULINA (Data Scientist, Government Transparency Institute).

ADMINISTRATOR RESPONSIBLE
Stefan SCHULZ

EDITORIAL ASSISTANT
Lyna PÄRT

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Budgetary Affairs
European Parliament
B-1047 Brussels
Email: Poldep-Budg@ep.europa.eu

Manuscript completed in June 2021
© European Union, 2021

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT
The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.
CONTENTS

LIST OF ABBREVIATIONS
LIST OF BOXES
LIST OF FIGURES
LIST OF TABLES

1 INTRODUCTION

1.1 Resume of study objectives
1.2 Background, Key Issues & Methodological Approach
   1.2.1 Background
   1.2.2 Key Issues
   1.2.3 Methodological Approach
1.3 Synopsis

2 IMPACT OF ORGANISED CRIME ON THE EU’S FINANCES

2.1 The most common forms of fraud affecting EU funding
2.2 Other ways in which criminal activity affects the EU’s finances
2.3 Proportion of EU’s finances that has been affected by fraud
2.4 Trends in the impact of organised crime on EU finances
2.5 Conclusions – Impact of Organised Crime on the EU Finances

3 EU & MEMBER STATE RESPONSES TO THE PROBLEM

3.1 EU Framework for Combating Organised Crime
   3.1.1 EU Strategy to tackle Organised Crime 2021-2025
   3.1.2 Directive (EU) 2017/1371 on the Fight Against Fraud to the Union’s
       Financial Interests by Means of Criminal Law (PIF Directive)
   3.1.3 European Court of Auditors 2019 recommendations
3.2 Member State approaches to tackling fraud
   3.2.1 What are the Common approaches and differences in legal frameworks,
       policies and strategies, and institutional structures in Member States?
   3.2.2 What are the shortcomings in the way Member States tackle organised crime’s
       attempts to defraud EU finances and funding programmes?
   3.2.3 How many investigations and prosecutions have taken place and what
       proportion have been successful? How much EU funding has been retrieved?
       What have been the problems in seeking to retrieve EU funds?
   3.2.4 Have the Commission’s tools to detect and tackle fraud been effective? Would
       increased use of these tools by Member States lead to better outcomes?
3.3 Conclusions – EU and Member State approaches to the problem
### LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFCOS</td>
<td>Anti-Fraud Coordination Service</td>
</tr>
<tr>
<td>ARCHNE</td>
<td>ARACHNE (database of EU-funded projects)</td>
</tr>
<tr>
<td>CAP</td>
<td>Common Agricultural Policy</td>
</tr>
<tr>
<td>CFP</td>
<td>Common Fisheries Policy</td>
</tr>
<tr>
<td>CF</td>
<td>Cohesion Fund</td>
</tr>
<tr>
<td>DG BUDG</td>
<td>Directorate-General for Budget</td>
</tr>
<tr>
<td>DG JUST</td>
<td>DG Justice and Consumers</td>
</tr>
<tr>
<td>TAXUD</td>
<td>Directorate-General Taxation and Customs Union</td>
</tr>
<tr>
<td>ECTS</td>
<td>European Credit Transfer System</td>
</tr>
<tr>
<td>EDES</td>
<td>Early Detection and Exclusion System</td>
</tr>
<tr>
<td>EP</td>
<td>European Parliament</td>
</tr>
<tr>
<td>ERDF</td>
<td>European Regional Development Fund</td>
</tr>
<tr>
<td>ESF</td>
<td>European Social Fund</td>
</tr>
<tr>
<td>ECA</td>
<td>European Court of Auditors</td>
</tr>
<tr>
<td>EPPO</td>
<td>European Public Prosecutor's Office</td>
</tr>
<tr>
<td>EUROJUST</td>
<td>European Union Agency for Criminal Justice Cooperation</td>
</tr>
<tr>
<td>EUROPOL</td>
<td>European Union Agency for Law Enforcement Cooperation</td>
</tr>
<tr>
<td>EMPACT</td>
<td>European Multidisciplinary Platform on Organised Crime</td>
</tr>
<tr>
<td>GDP</td>
<td>Gross Domestic Product</td>
</tr>
<tr>
<td>MTIC</td>
<td>Missing Trader Intra Community fraud</td>
</tr>
<tr>
<td>NAFS</td>
<td>National Anti-Fraud Strategy</td>
</tr>
<tr>
<td>OLAF</td>
<td>European Commission’s Anti-Fraud Office</td>
</tr>
<tr>
<td>PiF</td>
<td>Protection of the Financial Interests of the Union (Report)</td>
</tr>
<tr>
<td>SOCTA</td>
<td>Serious and Organised Crime Threat Assessment (Reports)</td>
</tr>
<tr>
<td>TNA</td>
<td>Transaction Network Analysis</td>
</tr>
<tr>
<td>VAT</td>
<td>Value Added Tax</td>
</tr>
</tbody>
</table>
LIST OF BOXES

Box 1.1: Key Study Questions 11
Box 2.1: Key Questions - Impact of Organised Crime on the EU’s Finances 15
Box 2.2: National level estimates of fraud 22
Box 2.1: Key Questions - EU & Member State Responses to the Problem 25
Box 3.2: Recent EU legislative measures to combat VAT fraud 27
Box 3.3: National Transposition of the PIF Directive 29
Box 3.4: National strategies to combat organised crime and fraud 31
Box 3.5: Role of the AFCOS in Member States 32
Box 3.6: Example - Defining organised crime in Italy 34
Box 3.7: Examples - Fighting fraud and organised crime in Member States 36
Box 3.8: Examples – Member State fraud data tools 40
Box 3.9: Transaction Network Analysis (TNA) 44

LIST OF FIGURES

Figure 2.1: Irregularities reported as fraudulent (including third countries (pre-accession) and direct expenditure (number of suspected cases) 200
Figure 2.2: Financial value (EUR) of irregularities reported as fraud 21
Figure 4.1: Predicted OC infiltration probabilities averaged by European NUTS3 regions, based on the sample of EU-funded contracts awarded by municipalities. 51

LIST OF TABLES

Table 3.1: Examples of prevention and detection actions 39
1 INTRODUCTION

1.1 Resume of study objectives

To summarise, the objectives of this study were to:

- Analyse the impact of organised crime and corruption on the EU’s budget and financial interests, particularly losses to the EU budget through criminal activities.
- Examine the differences and common approaches used by Member States to investigate organised crime and assess their effectiveness. This step will later involve investigating and quantifying how much costs could be reduced if Member States implemented best practice.

In relation to the first objective, the study was required to produce a ‘best estimate’, quantified as far as possible, of the potential losses to the EU budget that could be prevented or recovered if all EU-27 Member States implemented the best practice approaches identified to tackle organised crime. The analysis was also to examine the risks related to the infiltration of criminal organisations into the legal economy, bearing in mind the imminent entry into operation of the economic recovery tools to help mitigate the effects of the Covid-19 pandemic.

In terms of scope, the study examined both the expenditure and revenue sides of EU finances and the extent to which these different aspects are affected by fraud that is perpetrated by organised crime.

Although many aspects of the research cover the EU as a whole, the research involving Member States focused on a sample of 15 EU Member States (BG, CZ, DE, DK, ES, FR, GR, HU, LU, LT, NL, MT, PL, SE, SK). The sample was selected in consultation with the EP and designed to provide a representative spread in terms of a number of key variables (geography, use of EU funding, organised crime activity and national approaches to combating the problem). The original sample was smaller but expanded to include a number of other countries including the Czech Republic, Slovakia and Malta as there have been recent notable cases of organised crime and fraud and these countries are consequently of interest to the Budgetary Control Committee.

1.2 Background, Key Issues & Methodological Approach

Before turning to the study findings (Section 2), we first summarise the background to the study, the key issues that have been investigated, and explain how the research was carried out.

1.2.1 Background

As the EP emphasised in its terms of reference, the Commission and the Member States have a shared responsibility to protect the EU’s financial interests against fraud and corruption.

Article 325 of TFEU states: “The Union and the Member States shall counter fraud and any other illegal activities affecting the financial interests of the Union through measures to be taken in accordance with this Article, which shall act as a deterrent and be such as to afford effective protection in the Member States, and in all the Union’s institutions, bodies, offices and agencies. Member States shall take the same measures to counter fraud affecting the financial interest of the Union as they take to counter fraud affecting their own financial interest. Without prejudice to other provisions of the Treaties, the Member States shall coordinate their action aimed at protecting the financial interest of the Union against fraud. To this end they shall organise, together with the Commission, close and regular cooperation between their competent authorities”.

Over the last ten years, the Commission has taken steps to fight fraud against the EU budget. In particular, it adopted the ‘Commission Anti-fraud Strategy’ (CAFS) in 2011. Following a review in
2019, a priority agreed to equip the Commission with a stronger analytical capability and with a more centralised system of oversight to help identify, prevent and detect fraud against the EU’s financial interests. The Commission has also established an ‘Early Detection and Exclusion System’ (EDES), and an inter-institutional panel which advises on whether to exclude economic operators from EU financing. Each year, the Commission presents to the EP and the Council a report on the ‘Protection of the Financial Interests of the Union’ (the ‘PIF report’). The most recent initiative is the launch of the European Public Prosecutor’s Office (EPPO) which has been given responsibility for investigating, prosecuting and bringing to judgment crimes against the financial interests of the EU (i.e. various types of fraud, VAT fraud with damages above 10 million euro, money laundering, corruption, etc).

However, as noted in the terms of reference for this study, there is scope for further strengthening measures to combat fraud against the EU finances. Quoting a European Court of Auditors’ report, the Commission lacks comprehensive information on the scale, nature and causes of fraud in EU spending. Moreover, the Commission has not so far carried out any assessment of undetected fraud, nor detailed analysis of what causes economic actors to engage in fraudulent activities. In addition, fraud is thought to be closely linked with corruption, which is a key issue in several Member States, but in 2017 the Commission decided to discontinue its ‘EU Anti-Corruption Report’.

As this study shows, all the available evidence suggests that the scale of fraud against the EU finances is vast. This at first sight does not appear to be the case on the expenditure side but here there is a particular problem of identifying ‘missing’ funds. On the revenue side, estimates from the Commission suggest that the VAT gap amounted to EUR 150 billion in 2016, EUR 50 billion of which were defrauded by criminal groups. Other estimates highlighted below indicate potentially higher levels of fraud. Our estimates (explained in Section 2.3) indicate around EUR 2.0 billion to EUR 2.7 billion of EU finances is lost to organised crime. Considering the EU’s 2020 budget of EUR 165 billion, this is calculated to represent between 1% and 1.6% of the EU’s budget.

In this study, “EU expenditure” refers to EU funds provided through grants to Member States inter alia through the Common Agricultural Policy, and Cohesion Policy and Regional Funds. When it comes to “EU revenue”, the study focuses on VAT fraud and, to a lesser extent, customs and excise fraud. It should be noted that most of the VAT fraud is lost income to the Member States. The EU only receives a small percentage of VAT revenue (0.30% for all Member States, but a reduced amount of 0.15 % for Germany, the Netherlands and Sweden over the 2014-20 period). Furthermore, while customs duties also form part of the EU’s own resources, for the period of 2021-27 Member States will keep 25% of duties collected to help cover collection costs. Nonetheless, in this study, estimates of fraud in revenues include both the percentage of which that goes to Member States as well as the EU unless otherwise specified.

Although irregularities and unintentional misuse of funds (e.g. mistakes in completing forms to claim grants) undoubtedly account for some of the ‘missing’ funds, fraud can still represent a major part of these irregularities. This applies especially to the revenue side where the complexity of schemes to defraud EU finances is such that only organised crime has the capability of implementing such schemes. The Parliament’s terms of reference outline the EU’s strategy to

---

combat organised crime but there too, there is scope to strengthen measures specifically to tackle crimes against the EU finances.

Expenditure totalling €1.8 trillion is envisaged under the EU’s long-term budget, coupled with NextGenerationEU, the temporary instrument designed to boost the post-COVID-19 recovery. Given the scale of this stimulus package, the largest ever financed in Europe, and the need for funds to be disbursed quickly to have the desired impact, it is clearly important to identify ways of reducing the risk of fraud.

1.2.2 Key Issues

A number of key issues were defined in the EP’s terms of reference and these were further expanded by CSES in the inception paper. The list of key questions that have been investigated in the study is set out below.

**Box 1.1: Key Study Questions**

**Part A: Effects of organized crime on the EU’s finances**

1) What are the most common forms of fraud affecting EU funding? Which types of EU programmes are most affected in the country?

2) Beyond fraud, are there other ways in which criminal activity affects EU funding?

3) Is there an estimate of the proportion of EU funding that has been affected by fraud and other criminal activity? (Fraud through tenders and grants, VAT fraud, etc.)

4) What has been the trend in the impact of organised crime on EU finances – is the situation getting better, worse or staying the same? Are there notable differences between Member States?

**Part B: National approaches to tackling organised crime**

5) Are there any common approaches when it comes to legal frameworks, policies and strategies, and institutional structures in Member State(s) to combat organised crime? Are there any notable differences between Member States’ approaches?

6) What are the shortcomings in the way Member States tackle organised crime, specifically attempts to defraud EU finances and funding programmes? How can the shortcomings be best addressed?

8) How many investigations and prosecutions have taken place and what proportion have been successful? How much EU funding has been retrieved? What have been the problems in seeking to retrieve EU funds?

9) How well have different Member States performed when it comes to implementing the EU strategy for tackling organised crime?

10) Is there any early evidence indicating whether Transaction Network Analysis (TNA) tool has been effective in detecting and tackling VAT fraud?

11) Have the Commission’s tools to detect and tackle fraud, such as the Arachne IT platform or the Early Detection and Exclusion System (EDES), been effective in detecting and tackling fraud? Would increased use of these tools by Member States lead to better outcomes?
Part C: Cost savings from best practice in tackling organized crime affecting the EU’s finances

12) What approaches seem to work best in tackling the problem of organised crime, specifically in relation to financial crime? Why are certain approaches more effective than others?

13) What ‘best practice’ examples exist in Member States when it comes to tackling organised crime, specifically attempts to defraud EU finances and funding programmes?

14) To what extent could the losses to the EU budget be reduced if all Member States – and the EU itself – adopted ‘best practices’ in tackling organised crime?

15) To what extent are national authorities implementing the policies and measures developed at the EU level to help coordinate the response to the problem of organised crime and EU finances?

16) At an operational level, how well do Member States cooperate with the EU institutions (OLAF, etc)?

17) What measures (if any) are being taken to prevent organised criminal groups perpetrating fraud and other criminal activity in relation to the EU COVID-19 Recovery and Resilience Facility? Will existing national approaches to combating financial crime be sufficient?

18) What are the implications for the Recovery and Resilience Facility, in particular minimising the risk of organised crime groups perpetrating fraud? What ‘best practices’ should be adopted to help ensure that the EU expenditure under this facility is spent in the intended way?

1.2.3  Methodological Approach

The contract for this assignment was awarded on 17 March 2021. This was followed by preparation of an inception document and a meeting with the European Parliament on 30 March. Following this, CSES carried out desk research to examine material available at the EU level and in relation to the sample of 15 EU Member States. During the course of the study, a ‘country factsheet’ was completed for each country providing information on the scale and nature of fraud against the EU finances, existing strategies to combat the problem and where applicable, examples of good practice.

To support the desk research, we also carried out an interview programme. At the EU level, consultations were undertaken with the European Commission’s Anti-Fraud Office (OLAF), DG Justice, Europol, and the European Court of Auditors. OLAF provided CSES with contact details for the Anti-Fraud Coordination Service (AFCOS) contact points in the EU27 Member States and these were used as a starting point for the research in the sample of countries. We also invited all 85 AFCOS contacts to complete a short online questionnaire. In parallel with the AFCOS we identified a number of contacts ourselves in various countries. In total 43 stakeholders took part in the consultation programme.

An interim document was submitted to the European Parliament on 27 May 2021 setting out the results of the research at that point in the study. CSES also made a presentation to a workshop on ‘Missing Trader Fraud: definition, effects, prevention and solutions’ that was organised by the European Parliament on 26 May. Last but not least an internal workshop attended by 30 participants was organised by CSES on 7 July and CSES presented the study’s findings to the European Parliament’s Budgetary Control Committee on 12 July.
1.3 Synopsis

The study is structured as follows:

- **Section 2: Impact of Organised Crime on the EU’s Finances** – analyses the research feedback on the first of the key objective from the European Parliament’s terms of reference, i.e. to analyse the impact of organised crime and corruption on the EU’s budget and financial interests, particularly losses to the EU budget through criminal activities.

- **Section 3: EU & Member State Responses to the Problem** – examines the research feedback in relation to the second study objective, namely to assess the differences and common approaches used by Member States to investigate organised crime and assess their effectiveness in reducing the impact on the EU’s finances. Where relevant we highlight good practices.

- **Section 4: Modelling the Estimates of Fraud** – i.e. quantitative estimates of the impact of organised crime on EU finances, specifically the expenditure side and public procurement. This part seeks to address the problem of quantifying fraud affecting EU expenditure where there are fewer existing estimates than on the revenue side.

- **Section 5: Conclusions and Recommendations** - presents the overall conclusions and recommendations of the study.

There are several appendices: a list of secondary sources, a summary of the methodology for the modelling exercise and the country factsheets (Annex C, available as a separate document online only).
2 IMPACT OF ORGANISED CRIME ON THE EU’S FINANCES

This section analyses the research feedback on the first of the key objectives from the European Parliament’s, i.e. to analyse the impact of organised crime and corruption on the EU’s budget and financial interests, particularly losses to the EU budget through criminal activities.

The analysis is broken down into a number of sub-sections that address the following questions from the Parliament’s terms of reference:

**Box 2.1: Key Questions - Impact of Organised Crime on the EU’s Finances**

- What are the most common forms of fraud affecting EU funding? Which types of EU programmes are most affected in the country?
- Beyond fraud, are there other ways in which criminal activity affects EU funding?
- Is there an estimate of the proportion of EU funding that has been affected by fraud and other criminal activity? (Fraud through tenders and grants, VAT fraud, etc.)
- What has been the trend in the impact of organised crime on EU finances – is the situation getting better, worse or staying the same? Are there notable differences between Member States?

Below we examine these questions. The assessment is based on desk research to examine EU level documentation and the interviews with EU-level stakeholders.

2.1 The most common forms of fraud affecting EU funding

EU legislation defines fraud as a **deliberate infringement that is, or could be, prejudicial to the EU budget**.\(^4\) To understand the data reported by Member States to the Commission or detected by the Commission, it is essential to distinguish between fraud and other irregularities. An irregularity is any infringement of an EU provision by an economic operator which has, or would have, the effect of prejudicing the EU’s financial interests.\(^5\) The Member States are required to identify those reported irregularities in which they suspect fraud. Annex 4 to the **Guidelines for the elaboration of a National Anti-Fraud Strategy (NAFS)** also lists a number of fraud risks with regard to EU funds, their causes and potential consequences both at EU and national levels.\(^6\)

The SOCTA report provides an analysis of the different types of fraud:

**Subsidy fraud**: criminals submit fraudulent applications for EU grants or tenders. Typically, these applications are based on false declarations, progress reports and invoices used to justify public expenditure or the fraudulent award of public tenders and/or subsidies. Several of those we have interviewed have pointed out that such fraud can occur through spending projects of programmes such as in Cohesion Policy but also through other areas of EU expenditure including expenditure on R&D, agriculture and fisheries, and employment, all of which have experienced organised crime infiltration. Stakeholders we interviewed also indicated that infiltration of public procurement contracts by organised crime is a key source of such fraud. Some of those we consulted have noted that some of the Member States that tend to benefit the most from Cohesion Policy funding are also

---

\(^4\) European Court of Auditors (2019). *Tackling fraud in EU cohesion spending: managing authorities need to strengthen detection, response and coordination.*


\(^6\) Guidelines for the elaboration of a national anti-fraud strategy (NAFS)
countries within which fraud is a systemic problem. On the other hand, European Social Fund has been highlighted as being less liable to fraud as projects are mainly implemented through grants. There is significant administrative pressure involved for beneficiaries in justifying costs which make fraud less likely.

**Customs import fraud:** i.e. the false declaration of the value and origin of goods, and of the classification that applies to them. This type of fraud can be perpetrated by: undervaluing imported goods on import declarations, often using fraudulent documents; incorrectly declaring products imported to the EU by falsely declaring the category of goods according to the Integrated Tariff of the European Union or TARIC code in order to pay a lower duty rate; falsely declaring the origin of goods to circumvent anti-dumping duties imposed by the EU on a particular product from a specific country; dumping products on the EU market at a lower price than the normal value of the product.

**Excise Fraud:** this form of fraud takes advantage of different tariffs and taxation on goods travelling between Member States. Three prominent examples are outlined in the report:

- **Tobacco**: Price differences across Member States, and between Member States and neighbouring countries outside of the EU, are exploited by organised crime to make profits. VAT fraud in tobacco is another area in which organised crime is involved. Crime groups have been found to smuggle tobacco into Member States avoiding paying duties on these goods.

- **Oil**: Member States receive a large portion of their revenues from duties on oil products. Fraudsters can exploit the different tax rates applied between Member States for the same oil products. Another avenue for fraud is the different rates applied to different oil products such as heating or agricultural oils or diesel, the latter having a higher tax rate. These forms of fraud lead to losses in income for Member States amounting to billions of euros. The report also highlights that “an increasing shift to non-fossil fuels will create additional opportunities for fuel fraudsters”. Fraudsters can take advantage of biodiesel trading schemes by selling biofuels that have not been produced according to sustainability requirements.

- **Alcohol**: fraud schemes mainly target countries imposing comparatively high taxes on alcohol products. The SOCTA report for example notes that “alcohol is smuggled across the EU using excise duty suspension schemes”.

**VAT fraud:** this is defined as “avoiding the payment of VAT or fraudulently claiming repayments of VAT from national authorities following an illicit chain of transactions.” More details on VAT fraud are provided below. Those we interviewed indicated that the most common forms of VAT fraud are Missing Trader Intra Community fraud (MTIC fraud), e-commerce fraud, and fraud to the Customs Procedure 42.

There are of course many other instances of fraud but in most cases, these relate to programmes that are mainly supported by Member States. For example, social Benefit Fraud causes significant financial loss to the budgets of Member States and potentially deprives those genuinely in the need of aid from state support. Social benefit can entail fraud against medical insurance, employment benefits, unemployment allowances, or allowances for low-income workers and refugees. Another form of this fraud involves employees continuing to work while receiving unemployment benefits and receiving wages under the table from the employer. Although social benefit fraud is a serious problem, it does not involve major losses to the EU budget.

To illustrate the types of fraud affecting the EU budget in greater detail, the SOCTA report provides a number of case studies of recent crime network and scheme exposures. One case study on illegal cigarette factory in Spain—the first underground cigarette factory discovered in the EU — examines how over two million counterfeit cigarettes were “seized, produced in unsanitary conditions and with low quality components. The criminal network is estimated to make criminal profits of EUR
625,000 per week.” While this does not mention the impact of illegal cigarette production on the EU finances, the high profits indicate that similar networks could be amassing similar amounts of fraudulent income, which is diverting funds away from legitimate producers. This is a potentially significant loss to the industry as a whole. E-commerce, various types of internet services and emerging technologies have opened up the possibility of many new forms of fraud, especially where the underlying transaction is cross-border. 7

2.2 Other ways in which criminal activity affects the EU’s finances

Organised crime can be defined from three different perspectives. Considering the “crime” perspective, organised crime is a specific type of criminal activity characterized by a certain level of sophistication, continuity and rationality in contrast to sporadic and impulsive criminal behaviour.8 Putting the emphasis on the organisational aspect, organised crime can be defined as an operation of illegal business entities whose members are bound together because of their group interest and their desire to profit from illegal activity.9 Finally, another aspect focuses on the concentration of power or the alliance between criminals and political and economic elites. From this perspective organised crime denotes a systemic condition.10

Regarding other criminal activities that could affect EU finances beyond fraud, Article 4 of the PIF Directive defines and lists the offences affecting the financial interests of the EU:11

Money laundering: as described in Article 1(3) of Directive (EU) 2015/849 involving property derived from the criminal offences covered by this Directive constitutes a criminal offence.

Corruption: this can be both active and passive. Active corruption means the action of a person who promises, offers or gives, directly or through an intermediary, an advantage of any kind to a public official for himself or for a third party for him to act or to refrain from acting in accordance with his duty or in the exercise of his functions in a way which damages or is likely to damage the Union’s financial interests. While passive corruption is defined as the action of a public official who, directly or through an intermediary, requests or receives advantages of any kind, for himself or for a third party, or accepts a promise of such an advantage, to act or to refrain from acting in accordance with his duty or in the exercise of his functions in a way which damages or is likely to damage the Union’s financial interests. According to the Rule of Law Report, corruption can affect EU funding.12 It stresses that the fight against corruption has an important EU dimension as it is linked to the protection of the financial interests of the EU. The report acknowledges that although fraud and corruption are distinct legal concepts, fraud cases against the EU budget might involve corruption.13

Misappropriation: the PIF Directive also adds the designation of intentional misappropriation by a public official as a criminal offense. The term ‘public official’ is defined in a broad manner including not only individuals holding formal positions but also private persons involved in the management

7 Europol. (2021). Serious and organised crime threat assessment
12 The 2020 Rule of Law Report is the first annual report by the European Commission as part of the new European Rule of Law Mechanism announced in the Political Guidelines of President Von der Leyen. The aim of the report is to monitor significant developments relating to the rule of law across the EU as well as the specific situation in all the Member States. It aims to identify possible problems and best practices about the rule of law and to help Member States find solutions with support from the Commission and other stakeholders, such as the Venice Commission. The report aims to be a preventive tool, not a sanctioning mechanism or a recommendation report, although it could serve as the basis of further inspection of specific Member States.
of EU funds such as contractors. Inciting, aiding and abetting offenses against the financial interests of the EU, and the attempt to commit such offenses, are also designated as a crime. Besides fraud, a criminal activity highlighted as affecting EU finances is the illegal tobacco trade which is thought to account for €10 billion in lost public revenue each year for the EU and Member States.

In addition to the criminal offenses listed above, there are evolving forms of fraud against the EU’s finances. In particular, and as noted earlier, cybercrime is growing source of fraudulent activity. This consists of criminal acts committed online using electronic communications networks and information systems, such as the creation and spread of malware, hacking to steal sensitive personal or industry data, or denial of service attacks. Europol annually assesses the ‘Internet Organised Crime Threat’ and criminal offences driven by financial gain.14

In the case of misappropriation and money laundering, interviewees argued that these criminal activities are often intertwined with fraud of EU funds. For example, the proceeds of VAT fraud are typically transmitted via financial institutions in several countries to tax havens outside the EU where the authorities are less well-placed to identify illegal funds. The funds in question can remain hidden in these locations for several years before being transferred via legitimate schemes (e.g. property transactions) back to criminal organisations in the EU.

2.3 Proportion of EU’s finances that has been affected by fraud

There are a number of estimates of the proportion of EU funding that has been affected by fraud and other criminal activity. Precise estimates are of course impossible because of the nature of fraud which, by definition, is illegal and largely hidden. Our research suggests that estimates relating to EU expenditure tend to be less reliable than on the revenue side of the EU budget. Before giving our own estimate, we first review the various estimates identified through the desk research. As noted earlier, these vary considerably.

The European Commission’s 2019 ‘Annual Report on the Protection of the EU’s Financial Interests’ (PIF report15) notes that:

- Member States reported 11,726 irregularities (fraudulent and non-fraudulent) to the Commission (a decline of 2% since 2018) amounting to EUR 1.6 billion;
- This was a decline of 34% compared to 2018.16 The report argues that this decline indicates that Member States have implemented practices which have improved the detection of irregularities. It could, however, also reflect the fact that fewer irregularities are actually being detected;
- Of these irregularities, Member States reported 939 as being fraudulent (8% of irregularities) amounting to a financial sum of EUR 461.4 million (28% of the irregularities). In comparison, Member States reported 10,787 irregularities as non-fraudulent which amounted to EUR 1.2 billion.

---

15 OLAF’s annual report on the protection of the European Union’s financial interests provides an update on the legislative acts adopted by the EU institutions to protect the EU’s financial interests. The report provides an update on the measures being taken and proposed by the EU to tackle fraud as well as the measures taken by Member States. In the latter case, this includes updates on the transposition of the Directive on the fight against fraud to the Union’s financial interests by means of criminal law. The report also lists the operational organisational, and administrative measures being taken to improve their legal and institutional framework to tackle fraud. In addition, the report provides figures on the amount and financial size of fraudulent and non-fraudulent irregularities in EU revenues and expenditures.
16 European Commission, OLAF, Annual Reports on the protection of the EU’s financial interests ("PIF" Report).
The PIF report provides a breakdown of these data between EU expenditure and revenue. In relation to EU revenues, for the EU-28 (including the UK in 2019), in 2019 a total of 425 irregularities were detected as fraudulent, amounting to a sum of EUR 79,754,209 (in comparison, 4,237 non-fraudulent irregularities were detected amounting to a sum of EUR 397,118,464). In 2019, the number of detected fraudulent irregularities was 21% lower than the average of 541 for the period 2015-19 as a whole (the financial sum involved was 19% lower than the average for the 2015-19 period of EUR 98 million). The report further notes that cross-border value-added tax (VAT) fraud cases amounted to at least € 10 million in 2019. The latest OLAF annual report for 2020 indicated that OLAF detected EUR 293.4 million of fraud against EU expenditure and revenues.17

When it comes to EU expenditure, the PIF report indicates that 426 irregularities were detected in 2019 amounting to EUR 366,603,821 (compared to 4,623 non-fraudulent irregularities amounting to EUR 710,748,903). These expenditures related to agriculture, internal policies, as well as cohesion policy and fisheries.

The EU has reported serious shortcomings in the disbursement and management of these funds primarily due to recurrent or one-off cases of fraud and corruption in some Member States. Beyond the direct consequence of diverting taxpayers’ money away from their foreseen use, these shortcomings have more severe negative implications. For instance, they can lead to the realisation of poor-quality infrastructures and services endangering the EU citizens’ well-being and safety and eventually result in the long-term in a progressive erosion of the level of public trust towards the EU Institutions and funds in some Member States.

Tackling fraud and corruption affecting the EU funds is a great challenge primarily because of the lack of comprehensive data and information at EU level. The type of fraud and corruption schemes affecting ESI Funds greatly vary across the EU Member States. The OECD has identified several risks of fraud and vulnerabilities throughout the project lifecycle and highlights complex fraud and corruption schemes and tactics that might be typically operated by the perpetrators. Some of the identified risks and tactics that might arise at different stages of the ESI project lifecycle include: conflict of interest, bribery, collusive bidding, influence peddling, creating fictitious companies, manipulating or forging documents.18

The charts of the next page provide a summary of the number and value of irregularities in EU expenditure and revenue over the period since 2015. The first chart shows the downward trend but as argued earlier, it is not clear whether this reflects increasing success in tackling the problem of fraud against the EU finances or the fact that an increasing amount is going undetected. The second chart shows a marked fall in the value of fraud reported by the Member States between 2018-19 but suggests that this was relatively stable before then. Despite having detailed figures of the levels of fraud reported by Member States, the PIF report stresses that these are not necessarily the true levels of irregularities but a reflection of the ability of Member States to detect irregularities both fraudulent and non-fraudulent. Furthermore, the manner in which fraud is defined will also reflect the differing levels of reporting by some Member States compared to others.

A further important consideration is that not all fraud is committed by organised crime. This is especially so on the expenditure side where there are, for example, individuals who benefit from EU payments which in some cases could be claimed fraudulently. The same applies to business

17 OLAF. (2021). The OLAF report 2020
18 OECD, Fraud and corruption in European Structural and Investment Funds. A spotlight on common schemes and preventive actions (2019).
claims involving the European Regional Development Fund. The proportion of fraudulent irregularity committed by organised crime is, however, probably very high on the revenue side of the EU budget because of the complexity of fraudulent schemes (e.g. ‘Missing Trader Intra-Community’ fraud). Europol cites several estimates for the financial cost of fraud. Europol notes that organised crime tends to be behind most cases of VAT fraud because the schemes involved in order to carry it out is complex. When it comes to MTIC fraud, between EUR 40 billion to EUR 60 billion is lost per annum to organised crime groups. Furthermore, 2% of organised crime groups are involved in 80% of the MTIC fraud.\(^\text{19}\)

Another estimate indicates that MTIC fraud could have amounted to 94 billion euros in 2014.\(^\text{20}\) When it comes to cross-border e-commerce fraud committed through the exemption of low-value consignments, the Commission estimates that overall loses could be as high as EUR 5 billion per year.\(^\text{21}\) One contact we interviewed further noted that when it comes to excise fraud, around EUR 10 billion to EUR 15 billion is lost per year for the whole of the EU, although this figure is constantly changing. The most recent figures provided to us are EUR 8.5 billion fraud on tobacco products,\(^\text{22}\) EUR 4 billion for gasoline and oil products,\(^\text{23}\) and EUR 1.3 billion for alcohol products each year.\(^\text{24}\) Another indication, from the UK, is that VAT fraud amounts to some EUR 2 billion per annum in the UK. A significant factor is the growing proportion of VAT fraud associated with e-commerce which is now thought to account for somewhere between 8-12% of the VAT ‘gap’.\(^\text{25}\)

Figure 2.1: Irregularities reported as fraudulent (including third countries (pre-accession) and direct expenditure (number of suspected cases)

Source: Authors’ visualisation of data in PIF report


Below we examine the differences between EU expenditure and revenue fraud in further detail.

**Irregularities in expenditures**

The PIF report highlighted that in the *Common Agricultural Policy* area of expenditure, 235 cases of irregularities were reported as fraudulent in 2019 (a 3% drop) representing EUR 24.6 million (a -62% drop since 2018). This compared with the 2,798 irregularities reported as non-fraudulent (an increase in 1%) amounting to EUR 206.1 million (an increase of 32%). The report noted that the irregularities (particularly the fraudulent irregularities) were concentrated in a few Member states. The report does, however, point out that this could be due to the difference between Member States’ in their ability to detect and prevent fraud, as well as how they report it.

**Cohesion policy and fisheries** is the area of EU expenditure involving the most fraud. Here, the PIF report indicates that 187 irregularities were reported as fraudulent in 2019 (a drop of 43%) which amounted to EUR 338.8 million lost funds (a fall of 59%). This compares with the 1,812 cases reported as non-fraudulent (a fall of 6%) which amounted to EUR 502.4 million (a fall of -11%). On average, across the irregularities, the report found that the average amount of fraud was substantially larger than the average for irregularities reported as non-fraudulent. The ERDF saw the highest number of fraudulent irregularities.

Overall, the SOCTA report highlights how *corruption, ranging from petty bribery to complex multi-million-euro corruption schemes*, can weaken state institutions and finances. Even if internal corruption does not directly cause a loss of EU funds, it can cause imbalances in a Member States’ and the EU’s economy. Approximately 60% of the criminal groups identified in the SOCTA 2021 report engage in corruption. As the report states “by creating economic imbalances and market distortion, these criminal activities weaken the integrity of the national and international markets and financial systems and support the growth of underground economies.” Additionally,

---

26 The Member States that did not detect fraud were Belgium, Estonia, Ireland, Greece, Croatia, Cyprus, Luxembourg, Hungary, Malta, and Sweden.
the OECD notes that based on the estimated from previous detected fraud cases alone, over EUR 390 million every year is misappropriated from the structural funds. The box below provides estimates of fraud affecting EU expenditure and revenue by way of example in three EU Member States.

**Box 2.2: Examples of Member State estimates of fraud**

- **Finland**: fraud involving VAT refund requests under false pretences leads to losses of EUR 30 million per annum.27

- **France**: the financial impact of fraud and other illegal activities affecting the EU’s financial interest in France was estimated to amount to over EUR 4 million p.a. of expenditure and to over EUR 6 million p.a. in revenue by the European Commission.28 However, it should be noted that these estimates are likely to be underestimates. Regarding VAT fraud, according to the latest figures provided by the European Commission, in 2018 France lost EUR 12.7 billion p.a. of VAT revenue to fraud and evasion, tax avoidance, bankruptcies, financial insolvencies and miscalculations.29 More recent estimates provided by the French Court of Audit (Cour de Comptes) estimate the losses incurred due to VAT fraud to be around EUR 15 billion in 2019.30

- **Italy**: in 2019, the total value of irregularities including fraud is estimated to have amounted to EUR 16.1 million from a total of 103 reported cases in the IMS database for Cohesion Policy. Looking at the breakdown by type of fund, the ERDF reported the highest number of irregularities (71%). OLAF estimated that for that year the withdrawn amounts were worth about EUR 12 million.31

**Irregularities in revenues**

In 2019, irregularities in EU revenues mainly affected customs duties. The method used to detect fraud in revenues was through post-release controls while the most successful methods to detect fraud were inspections by anti-fraud services. Furthermore, post-release controls were noted as being important for tackling organised crime involvement in evasion of duty fees and new issues in fraud such as undervaluation.

Although the SOCTA report does not provide detailed estimates on the financial impact of each type of fraud, it does mention how customs import fraud resulted in financial losses of at least EUR 5.5 billion to the EU budget between 2016 and 2019. It also estimates that up to EUR 50 billion is lost due to the activities of VAT fraudsters every year.

Between 2017-19 the Commission inspected the control strategies employed by Member States for customs checks and found many to be insufficient to protect the EU’s financial interests. So far, OLAF has provided investigative reports with recommendations to five Member States (Czech Republic, France, Greece, Hungary, Malta, and Slovakia) but the 2019 PIF report notes that when it

---

31 The definition attributed to the term “Withdrawal” consists of “withdrawing irregular expenditure from the program as soon as it is detected, deducting it from the next interim payment application, thus making EU funding available to other operations”. In practice, the definition of “withdrawal” is essentially the same as the so-called “decertification” in the Italian reports, which allows the elimination of expenses for projects that are no longer strategic or where irregularities or fraud against the EU budget have been detected.
comes to measures to prevent and detect undervaluation fraud, all Member States have deficiencies in the measures employed.

Taken together, fraud involving organised crime can be estimated to amount to around EUR 2.0 billion to EUR 2.7 billion per annum, equivalent to between 1% and 2% of the EU’s 2020 budget. The calculation is set out below:

Box 2.3: Own ‘consensus’ estimate of the impact of organised crime on the EU’s finances

- The EU’s budget for 2020 was EUR 165.8 billion.
- The quantitative model we have used (see Section 4) indicates that EUR 1.9 billion to EUR 2.6 billion could be lost to organised crime in EU expenditures.
- On the revenue side, MTIC fraud involving organised crime groups is estimated by the Commission to be around EUR 40 billion to EUR 60 billion per annum.
- Taking EUR 50 billion as a base estimate, and assuming a uniform call rate of 0.3% (in reality this varies as discussed above), the EU itself is likely to incur losses of EUR 150 million of VAT revenues that can be attributed to organised crime groups (0.3% of EUR 50 billion).
- Adding together the estimates of the EU expenditures and VAT revenues lost to organised crime and the expenditures, we arrive at around EUR 2.0 billion to EUR 2.7 billion p.a. of EU finances is lost to organised crime.
- This amounts to between 1% and 2% of the EU’s budget of EUR 165.8 billion for 2020 budget.

2.4 Trends in the impact of organised crime on EU finances

In some areas of organised criminal activity, the situation is getting worse. This is the case for fraud, drug trafficking and counterfeiting. The research feedback suggests that around 60% of organised crime groups use corruption as a tool for criminal activity and 80% of organised crime groups use shell companies. Similarly, the SOCTA report indicates that fraud perpetrated by organised crime and is getting worse, particularly when it comes to transnational crime.

The SOCTA report also argues that (as highlighted earlier) organised crime in the EU relies on the ability to launder criminal profits to ensure that fraud remains undetected. For this purpose, professional money launderers have established a parallel underground financial system to process transactions that is largely beyond the reach of oversight mechanisms governing the legal financial system. Underscoring the SOCTA report’s findings is the warning that criminal networks are adaptable and flexible in evading new measures and changes in legislation, the economic situation and law enforcement actions. The fraudulent schemes of criminal networks are constantly evolving and improving in order to take advantage of the weaknesses of the state and legislation.

The Covid-19 pandemic has also created more opportunities for fraudsters and organised crime. The SOCTA report warns that “a potential deep economic recession following the pandemic will fundamentally shape serious and organised crime in the EU for the near future. Previous periods of economic stress can provide some degree of insight into how these developments might affect crime in the EU and what responses need to be formulated to counter existing and emerging threats to the EU’s internal security during this time.” However, there are several factors to be mindful of. For example, it is expected that some criminals will specialise in abusing recovery and support schemes by orchestrating complex networks of companies in order to defraud public funds. The
potential loss of billions of euros of public revenues through VAT and other frauds directly affects taxpayer interests and the ability of governments to fund essential public services. Among EU citizens, it is argued that rising unemployment and further constraints on the budgetary resources of public authorities may present greater opportunities for criminal groups, as individuals and organisations in the private and public sectors are rendered more vulnerable to compromise.

Similarly, the 2019 PIF report noted that there is a risk that the COVID-19 crisis could lead to an increase in fraud in the health care sector. The report notes this as a point of concern as 15 EU Member States reported irregularities in 2019 in health infrastructure and seven of these also detected fraud. In these cases, more than half of the fraudulent irregularities were declared by Romania and Slovakia, and a third was reported by Poland. In terms of the scale of the fraud, Slovakia reported fraud amounting to half of the total fraudulent irregularities.

The study research suggests that some of the Member States that benefit the most from Cohesion and Regional Development funds are also countries within which fraud is a systemic problem. On the other hand, other factors such as their geographical location can influence the extent to which organised crime tend to be involved in different Member States. For example, if a Member State has a port, it is more likely to be a target for organised crime involving trade, and if the Member State has a large economy and financial sector it can be at particular risk of money laundering as these funds can be hidden within a larger economy more easily than in a smaller one.

### 2.5 Conclusions – Impact of Organised Crime on the EU Finances

This section has highlighted estimates of the losses to the EU’s finances that are thought to be associated with fraudulent activities. Our estimates indicate around EUR 2.0 billion to EUR 2.7 billion of EU finances, both expenditures and revenues, is lost to organised crime. Considering the EU’s 2020 budget of EUR 165.8 billion, this represents between 1% and 2% of the EU’s budget.
3 EU & MEMBER STATE RESPONSES TO THE PROBLEM

Section 3 examines the research feedback in relation to the second study objective, namely to assess the differences and common approaches used by Member States to investigate organised crime and assess their effectiveness in reducing the impact on the EU’s finances.

The research draws on a combination of desk research and interviews. The assessment is supported by country factsheets for each of the Member States in our sample for this study (see Annex B). As noted in Section 1, the research focused on a number of questions:

Box 3.1: Key Questions - EU & Member State Responses to the Problem

- Are there any common approaches when it comes to legal frameworks, policies and strategies, and institutional structures in Member State(s) to combat organised crime? Are there any notable differences between Member States’ approaches?
- What are the shortcomings in the way Member States tackle organised crime, specifically attempts to defraud EU finances and funding programmes? How can the shortcomings be best addressed?
- How many investigations and prosecutions have taken place and what proportion have been successful? How much EU funding has been retrieved? What have been the problems in seeking to retrieve EU funds?
- How well have different Member States performed when it comes to implementing the EU strategy for tackling organised crime?
- Is there any early evidence indicating whether Transaction Network Analysis (TNA) tool has been effective in detecting and tackling VAT fraud?
- Have the Commission’s tools to detect and tackle fraud, such as the Arachne IT platform or the Early Detection and Exclusion System (EDES), been effective in detecting and tackling fraud? Would increased use of these tools by Member States lead to better outcomes?

3.1 EU Framework for Combating Organised Crime

There are a number of elements to the EU’s framework for combating organised crime in relation to the EU’s finances. Within the European Commission, OLAF, DG BUDG, DG TAXUD and other DGs with a role in administering the Cohesion and other major expenditure programmes (DGs EMPL, AGRI, RTD, REGIO) all have a role. EUROPL, the ECA, Eurojust and the EPPO are all key elements. The EU’s Strategy to tackle Organised Crime 2021-25 and the Directive (EU) 2017/1371 on the Fight Against Fraud to the Union’s Financial Interests by Means of Criminal Law (the PIF Directive) provide an overall framework.

3.1.1 EU Strategy to tackle Organised Crime 2021-2025

The EU Strategy to tackle Organised Crime 2021-25\(^{32}\) aims to reinforce the response to serious organised crime by “boosting law enforcement and judicial cooperation, tackling organised crime structures and high priority crimes, removing criminal profits and ensuring an effective response to technological developments”.\(^{33}\) It outlines measures and tools to disrupt and combat international organised crime whilst reinforcing existing frameworks and initiatives to its fullest potential.


As part of the broader EU Security Union Strategy, the Strategy on Organised Crime highlights the key role of effective financial investigations in tackling priority crimes and of strategic information exchange to disrupt and dismantle relevant networks. It further stresses the need for Member States to collaborate on strategic and operational aspects, for example through the EU funded Operational Network (@ON) to target networks that pose the highest risk and to strengthen their collaboration efforts with Europol. In addition, it aims to maximise the potential use by Member States of the European Multidisciplinary Platform on Organised Crime (EMPACT), an EU flagship project with additional funding and suggests the creation of a new Police Cooperation Code that consolidates the rather fragmented legal framework on cross-border police cooperation and allows for partnerships across Member States.

Beyond the EU borders, the strategy proposes to reinforce international cooperation with non-EU countries and a cooperation agreement with Interpol to exchange timely information. Making the judiciary and law enforcement fit for the digital age is also a crucial measure. Data retention, encryption of information and encouraging the participation of Member States in the e-Evidence Digital Exchange System will be efforts carried out by the Commission, while Europol and CEPOL prepare tools and training for the relevant authorities.

The EU’s strategy is supported by the Serious and Organised Crime Threat Assessment (SOCTA) reports, a Europol analysis of the serious and organised crime landscape that provides lessons for relevant law enforcement agencies, decision-makers, and the wider public.

As a threat analysis, SOCTA has a particular focus on organised crime, including activities that target EU finances. Through the use of both quantitative and qualitative methods, a database comprised of inter alia nearly 4,000 records on criminal activities and networks. Based on these and other tools, Europol identifies the most prevalent, threatening criminal phenomena in the EU, and develops measures for combating these threats. The 2021 report focuses on cross-cutting issues that enable criminal activity, as well as the role of criminals within criminal processes. A recurring theme throughout the report is the pivotal role technology is playing in organised and serious crime, as well as increasing criminal networks’ ability to circumvent laws and frameworks. It argues that increased Internet usage in Member State can more easily connect criminals to potential victims, and the burgeoning marketplaces on the dark web, as well as other platforms, provide many resources for criminals to carry out various forms of fraud and scams.

3.1.2 Directive (EU) 2017/1371 on the Fight Against Fraud to the Union’s Financial Interests by Means of Criminal Law (PIF Directive)

The Directive (EU) 2017/1371 on the Fight Against Fraud to the Union’s Financial Interests by Means of Criminal Law (PIF Directive) was adopted as part of the Commission’s Anti-Fraud Strategy to strengthen the protection of the EU budget. The Directive aims to increase the level of protection of the EU budget by establishing common definitions of criminal offences against the financial interests of the EU and introduces minimum rules for sanctions and limitation periods, thereby harmonising the prosecution of offenses. The PIF Directive should have been transposed by EU Member States by the end of 2019 but even though this happened, it is not clear to what extent all Member States have put its various provisions fully into effect.

In the Directive, the definition of criminal offences covers active and passive fraud, as well as the misuse of funds. The Directive lays down minimum penalties for natural persons and establishes limitation periods that make it possible for the law to apply over a sufficient time to ensure that infringements can be addressed in an effective way. The Directive also introduces an obligation for the Member States, the Commission, the agencies and the Court of Auditors to cooperate. In addition, it
lays the foundation for the new **European Public Prosecutor’s Office** (EPPO), which is an independent and decentralised prosecution office of the EU with the competence to investigate, prosecute and bring to judgment crimes against the EU budget. According to the Commission’s Rule of Law report, the EPPO should play an important key role in harmonising the approach to fight fraud against the EU budget. Before the creation of the EPPO, the competence to investigate and prosecute fraud against the EU budget remained solely with the Member States. The EPPO has the competence to investigate, prosecute and bring to judgment in relation to crimes against the EU budget, such as fraud, corruption or serious cross-border VAT fraud.

The PIF Directive seeks to **harmonise the sanctions for crimes against the EU’s financial interests** by requiring Member States to introduce prison sentences of at least four years (“minimum maximum sanctions”) when the offences involve damage or advantage exceeding €10,000. For lesser offences, Member States may provide for punitive measures other than criminal sanctions. The PIF Directive provides only minimum rules and that Member States are therefore free to adopt more stringent rules for crimes against the EU’s financial interest. Regarding organised crime, Member States should consider an aggravating circumstance if the offenses are committed within a criminal organization as defined by Council Framework Decision 2008/841/JHA.34

Further measures in the Directive are designed to ensure that national policies (i) articulate the programme authorities anti-fraud and anti-corruption objectives in relation to specific operational programmes; (ii) clearly define roles and responsibilities relating to the fraud and corruption risk management; (iii) set clear reporting and investigation procedures and steps; (iv) define how the fraud risk management framework will be monitored. Member States should also ensure that the **programming authorities have the right set of skills and experience to conduct fraud risk assessment** and are periodically provided with ad-hoc training. Finally, the use of all available sources of information and databases and the use of data analytics techniques might help reinforce the Member State capacity to anticipate fraud risks at the earliest stages of the project lifecycle.

The PIF Directive also requires Member States to implement a limitation period of at least five years for the prosecution of serious criminal offenses against the financial interests of the EU, which trigger a maximum imprisonment of at least four years.

### Box 3.2: Recent EU legislative measures to combat VAT fraud

- An amendment of the VAT Directive35 was made in February 2020 to combat the issue of e-commerce VAT fraud. This amendment sought to strengthen the cooperation between tax authorities and payment service providers. The deadline for transposition is the 31 December 2021.

- Furthermore, an amendment of the administrative cooperation Regulation36 set up a central electronic system of payment information (‘CESOP’) allowing Member States to provide it payment information they store in their national level databases.

### 3.1.3 European Court of Auditors 2019 recommendations

In 2019, the European Court of Auditors also proposed measures to help reduce fraud against the EU finances. This included putting in place robust reporting system based on the Irregularity Management System (IMS); better coordination in tackling fraud based on fraud prevention and detection; the Commission should intensify its fraud prevention activities; increased use of the early

---

34 Council Framework Decision 2008/841/JHA
detection and exclusion system (EDES) by DGs and Member State; all Member States to make use of the Arachne database to prevent fraudulent and irregular use of EU funds; and reconsidering OLAF’s role and responsibilities in combating fraud in EU spending in light of the establishment of the EPPO, giving OLAF strategic oversight role in EU anti-fraud action.

3.2 Member State approaches to tackling fraud

In this sub-section we assess the differences and common approaches used by Member States to investigate organised crime and assess their effectiveness in reducing the impact on the EU’s finances.

3.2.1 What are the Common approaches and differences in legal frameworks, policies and strategies, and institutional structures in Member States?

The approach to tackling organised crime varies across Member States in terms of legislative framework, strategies in place and effective operational capacity. This rather fragmented situation is partially a result of Member States adding to EU legislation - such as the 1990 Convention implementing the Schengen agreement and the 2008 Prüm framework on combating terrorism and cross-border crime - with bilateral and multilateral agreements, which create uneven cooperation among countries and operational inefficiencies in cross-border cooperation.

This situation is further reinforced by the varying level of adoption and implementation of EU legislation, for example the EU rules regarding non-cash means of payment, the Directive on facilitating access to financial information, and the Council of Europe Medicrime Convention on counterfeit of medical products, which has been signed by 14 Member States of which only 6 have ratified it. Only some countries have developed a specialised strategic approach to specific topics such as combating environmental crimes and the same applies to enforcement and prosecution bodies at national level, which if existent often have divergent capacity and resources.37

Problem of corruption at a national level

The European Commission’s Rule of Law Report analysed the national approaches to fight against corruption, which as the report notes, is a key enabler to organised crime and is almost certainly linked to fraud cases against the EU budget. The report found out that several EU Member States have good national anti-corruption strategies in place or are at least developing them. Some Member States have also implemented reforms to strengthen corruption-prevention. Other countries have strengthened the capacity of the criminal justice system to fight corruption.

For example, Luxembourg has established an intergovernmental consultative Corruption Prevention Committee within its Ministry of Justice.38 However, some concerns were raised our consultations regarding the impunity of high-ranking officials, as well as problems with the complexity of investigating financial and economic crimes, and a lack of verification and enforcement for integrity measures. For instance, Czechia was pointed out as one of the Member States that does not pursue systematically high-level corruption cases, and where investigations and audits are currently ongoing at both national and European level into potential conflicts of interests and the use of EU funds.

To take further examples, in the case of Spain, the National Strategy against Serious and Organised Crime 2019-2023 sets the objective of dismantling criminal structures and reducing their impact on society by reducing their activity, while preventing the setting up of new groups and improving interagency cooperation, for example between the Police and the Civil Guard. This is linked to the National

37 EU Strategy to tackle Organised Crime 2021-2025
Security Strategy 2017 as the main overall national framework, which highlights organised crime and its destabilising force as one of the main threats to national security. In 2020, the French government created an inter-ministerial anti-fraud coordination mission (MICAF) tasked with the coordination of public administrations and other public bodies in the fight against fraud affecting public finances (compulsory tax and social deductions, social benefits) at the national and local levels.39

Implementation of the PIF Directive

As noted above, all EU Member States have now transposed the PIF Directive, albeit with differences in terms of the types of measures adopted in practice. Some examples of the measures taken to implement the PIF Directive’s provisions are provided below.

**Box 3.3: Examples - National Transposition of the PIF Directive**

- **France:** The government issued an ordinance (No 2019-963) which transposes the Directive into national law. While French criminal law partially met the requirements of the PIF Directive, the full transposition required the adoption of provisions relating to the jurisdiction of the courts, the aggravation of certain offenses and finally, the creation of an offence relating to intentional customs fraud.

- **Germany:** Germany transposed the PIF Directive into national law in June 2019.40 Although German law was considered to be broadly compliant with the requirements of the Directive at the time, the new law aimed to strengthen “the protection of the financial interests of the EU” (EU-Finanzschutzstärkungsgesetz – EUFinSchStG)41. It does so, among others, by regulating the offences of misapplication of funds or assets from the European Union budget managed by the Union and those of illegal diminution of the resources of the Union budget managed by the Union.

- **Italy:** The Italian government adopted the Legislative Decree No. 75 on 15 July 2020 in order to implement the ‘PIF Directive’. The Decree became effective on 30 July 2020 and introduced some changes to the Decree No. 231 of 8 June 2001 that provided for a direct liability of legal entities, companies and associations for certain crimes committed by their representatives. In particular, the Decree no. 75 introduced sanctions for the criminal actions against the financial interests of the EU42 and outlined new criminal offences leading to corporate liability such as: undue perception of disbursements; extortion; embezzlement; computer fraud to the detriment of the State or a public body; fraud in public supplies. The sanctions against fraud is also defined by specific provisions of the penal code43.

Italy is one of the few Member States that have adopted a National Anti-fraud Strategy and the Italian AFCO (COLAF) submits every year a Report to the Parliament to provide an overview of the situation and the priorities in the fight against fraud, the measures taken, the results achieved and the anti-fraud action to protect the economic and financial interests of the EU.44 Recently, Italy has issued new guidelines on how to communicate to the European Commission irregularities and fraud against the European budget that addresses possible critical elements in the communication of data concerning cases of irregularity/fraud against the EU budget to OLAF. Finally, the Italian authorities have adopted specific anti-fraud measures to protect resources and the interests of the Union, e.g. implementation and use of the ARACHNE tool, operational measures to detect irregularities/fraud and fight financial OC, operational plans to combat

---

39 [https://www.economie.gouv.fr/micaf](https://www.economie.gouv.fr/micaf)
40 [https://www.buzer.de/gesetz/13459/index.htm](https://www.buzer.de/gesetz/13459/index.htm)
42 Article 5 (2).
43 Articles 640 bis., 316 bis, 316 ter, art. 640 quarter and 322 ter.
44 The 2019 Annual Report was presented on 18 November 2020 [link](https://www.buzer.de/gesetz/13459/index.htm).
embezzlement, undue requests for and/or receipt of EU funds and VAT fraud. Italy makes use of the EU databases for irregularities and fraud (IMS) and national anti-fraud databases.

- **Malta**: adopted a National Anti-Fraud and Corruption strategy in 2008, which takes into account the need to structure to coordination between administrative and criminal checks and investigations. Malta has fully implemented the recommendation to strengthen its risk analysis to detect irregularities and fraud and tailored this analysis to different types of expenditure. 45 Malta also transposed provisions from the PIF Directive via an Amendment to Subtitle III of the Criminal Code. Subtitle III addresses numerous forms of fraud and punishments. 46 However, it is important to note that in the most recent PIF report, Malta admitted it had not made any assessment of the impact of its National Anti-Fraud Strategy on protecting the EU’s financial interests. 47

- **Spain**: fraud involving EU funds was included in 2019 in the Spanish Criminal Code (LO 1/2019, Title XIV, art. 308) as a result of transposing the PIF Directive into national law. As such, fraud of public aid and subsidies for both national and European funds is now jointly regulated in one same article 48. This same legislation regulates the application of administrative sanctions and establishes the possible criminal proceedings and the sanctions that can be imposed.

**National Anti-Fraud Strategy (NAFS)**

The European Commission has encouraged Member States to develop a National Anti-Fraud Strategy (NAFS), a measure embedding anti-fraud actions for the management of EU Funds to ensure coordinated practices at national level. 49 The NAFS can also include actions to protect both the EU and national budgets. 50 The model for the NAFS proposed by the Commission consists of five main sections namely: a state of play and fraud risk assessment; objectives and performance indicators; an action plan including measures to be implemented; and defining how the strategy will be evaluated and implemented. 51

As part of their NAFs, some countries have developed formal channels through which to engage the wider public in the fight against fraud and organised crime through the reporting of irregularities. This is the case, for example, with the National Anti-fraud Coordination Service in Spain, which opened an online communication channel in 2017 in relation to projects or operations financed with EU funds. This channel aims to serve as additional means of identifying irregularities and to allow the public authorities to carry out the corresponding investigations. 52 France adopted in 2016 a national anti-fraud strategy, as encouraged by the European Commission 53. This national strategy was developed to coordinate the fight against fraud in public finance and was adopted by the national committee against fraud (CNLF), after having been developed by the national delegation for the fight against fraud (DNLF).

---


49 See Guidelines for the elaboration of a national anti-fraud strategy (NAFS) (europa.eu)


51 Ibid.

52 https://www.iqae.pap.hacienda.gob.es/sitios/iqae/es-ES/snc/Paginas/ComunicacionSNCA.aspx

53 http://www.senat.fr/rap/r18-674/r18-674_mon_html%23toc71
It offers a roadmap aimed at combating fraud affecting national and EU funds, and as such integrated the issue of fraud against European funds within a comprehensive national strategy.

Joint initiatives in **Germany** between the federal authorities, civil society and the private sector have contributed to collective action against corruption risk, also in third countries. For example, ‘Alliance for Integrity’[^54] is a platform that offers solutions to strengthen the compliance capacities of companies, fosters dialogue between public and private sectors and creates a system of incentives for companies to increase their efforts against corruption in their own business environments.

**Box 3.4: Examples - National strategies to combat organised crime and fraud**

- **France**: the French government created in 2020 an inter-ministerial anti-fraud coordination mission (MICAF) tasked with the coordination of public administrations and other public bodies in the fight against fraud in public finances (compulsory tax and social deductions, social benefits etc.) at the national and local levels. MICAF also facilitates cooperation with the EU bodies responsible for protecting the financial interests of the European Union and in particular operational exchanges with the European Anti-Fraud Office (OLAF).

- **Latvia**: a second national antifraud strategy was approved by the Latvian government for the period 2020-2022 and seeks to enhance, *inter alia*, the exchange of information and cooperation between the Latvian AFCOS and OLAF, improve the representation of the Latvian AFCOS and participation in events and meetings organised by OLAF and the European Commission and foster the cooperation with the European Public Prosecutor’s Office. In addition, the implementation of the law “On Support to the European Anti-Fraud Office” is being complemented by the development of a manual of procedures for the effective implementation of this piece of legislation.

- **Spain**: the National Strategy against Serious and Organised Crime 2019-23 sets the objective of dismantling criminal structures and reducing their impact on society by reducing their activity, while preventing the set-up of new groups and improving inter-agency cooperation, e.g. between the Police and the Civil Guard. It is linked to the National Security Strategy 2017 as the main overall national framework, which highlights organised crime and its destabilising force as one of the main threats to national security. The National Anti-Fraud Strategy is expected to be developed from June 2021 onwards with the technical assistance from the Organisation for Economic Co-operation and Development (OECD).

**Role of the AFCOS**

In accordance with Article 12a of Regulation 883/2013, Member States are required to designate an **anti-fraud coordination service** (‘AFCO’) to “facilitate effective cooperation and exchange of information, including information of an operational nature” with OLAF. Member States may choose which body or authority is best placed to fulfil the role of AFCO. In many cases, the Ministry of Finance or the Ministry of Interior with high visibility and competence in the field of the protection of the EU financial interests are designated for this role. The EU legislation provides a high-level description of the mandate and tasks of the AFCOs.

As a minimum, AFCOs should ensure **co-operation with OLAF** pursuant Article 325 of the Treaty on the Functioning of the EU. In particular, upon the request of the Office, the AFCOs are expected to “provide or coordinate the necessary assistance for the Office to carry out its tasks effectively”[^55] throughout the course of an investigation. Furthermore, the national anti-fraud coordination services

[^54]: [https://www.allianceforintegrity.org/](https://www.allianceforintegrity.org/)
[^55]: Article 12a (2) Regulation 883/2013.
should have the **mandate to coordinate the legislative, administrative and investigative activities related to the protection of the EU’s financial interests**, as appropriate. AFCOs may also support OLAF in conducting **horizontal cooperation activities and exchange of information** between anti-fraud coordination services. In practice, the mandate and activities carried out by the AFCOs vary depending on the country-specific needs, anti-fraud strategy and other circumstances. These activities might include for instance: cooperation on investigations with OLAF, performing on-the-spot checks, facilitating cooperation between national administrations and OLAF, developing and implementing national strategies to protect EU’s financial interests.

The table below provides some examples of relatively proactive AFCOs with strong investigative and coordination powers and, on the other hand, less proactive services.

**Box 3.5: Examples - Role of the AFCOS in Member States**

- **Germany:** The Division for the Protection of EU Financial Interests (Division E A6) under the Ministry of Finance is the designated Anti-Fraud Coordination Service (AFCOS) in Germany. It also covers EU financial control and fraud prevention and EU regulatory and executive agencies.

- **Malta:** The Maltese AFCOS is located within the Internal Audit and Investigations Department (IAID). This enables it to conduct internal audits within all governmental departments and agencies and keep these authorities in check. The IAID conducts joint investigations with OLAF on all EU funds Malta avails of.

- **Luxembourg:** The Directorate of International Financial Relations serves as the AFCOS. This Directorate is comprised of three divisions: European Affairs, International Economic Policy, and Bilateral Relations and Regional Cooperation. For international economic policy, the Directorate defines and represents such policy in the EU, WTO, OECD, UNCTAD, and UNCITRAL, as well as represents Luxembourg in international for a on common commercial policy. In cases of suspected fraud followed by an investigation, this Directorate is kept abreast on the exchanges between relevant managing authorities, OLAF and the Public Prosecutor’s Office.

- **Italy:** the National Committee to combat fraud against the European Union ("COLAF") serves as the AFCOS for Italy. The Committee consists of high-level representatives of all administrations responsible for the management of the EU funds and fraud control. It is also supported by a technical secretary coordinated by a specific anti-fraud division of the Italian Economic and Financial Police ("Guardia di Finanza"). The Committee is mandated to coordinate all national activities to prevent and combat fraud and irregularities relating in particular to tax, CAP and structural funds. It is also the contact point of the Advisory Committee for the Coordination of Fraud Prevention (COCOLAF) of the Commission and the Working Group on combating Fraud of the European Council.

- **France:** The inter-ministerial anti-fraud coordination mission (MICAF) acts as the French AFCOS. As such, MICAF works with OLAF to facilitate its investigations by ensuring, for example, that it gains access to bank accounts in order to effectively undertake its investigations. MICAF also collaborates with the European Public Prosecutor’s Office. However, MICAF does not have any investigative powers and only acts as an interface and coordinator for the 10 national working groups tasked with several aspects of fraud. In addition, MICAF’s core mission and responsibilities are found in the fight against fraud at the national and regional levels.

---

56 Anti-fraud coordination service (AFCOS) | European Anti-Fraud Office (europa.eu)
57 Article 12a (3) Regulation 883/2013.
• **Poland**: The AFCOS of Poland serves as a central national contact point for issues related to expenditures as part of shared management. The role of the national AFCOS in this case is limited to serving as an intermediary between OLAF and competent national authorities. It coordinates and forwards OLAF requests and seeks to ensure a proper flow of reliable information. The AFCOS in Poland can provide OLAF with information, support, additional explanations and documents necessary at their request for OLAF’s administrative investigations. When it comes to EU revenues, other bodies have been appointed to cooperate with OLAF. The fight against organised crime, corruption and fraud are the responsibilities of national law enforcement authorities such as the police, anti-corruption and prosecutor’s services, and the revenue service when it comes to VAT and customs. In Poland, there is no legal distinction between the protection of national funds and EU funds.

• **Slovakia**: National Office for OLAF is operating as ‘Section of Control’ in the Office of the Government of the Slovak Republic. The role of the National Office is ensuring and coordinating the financial interests of the EU in Slovakia. It provides assistance to OLAF, and the representatives of the office are present on the on-the-spot checks, which is considered one of their main tasks. The office also coordinates an active network, coordinates and disseminates information, and provides training. They also report irregularities but only those that need to be reported to OLAF. The office has responsibilities under shared management. On the revenue side they do not have much information and there they are not directly involved in the reporting either.

### 3.2.2 What are the shortcomings in the way Member States tackle organised crime’s attempts to defraud EU finances and funding programmes?

The fight against fraud in the EU is very dependent on the activities of Member States. **OLAF has investigative powers when it comes to fraud and protecting the EU’s financial interests but it can only recommend Member States to carry out investigations and prosecutions, and cannot perform prosecutions itself.** This situation has changed with the establishment of the EPPO which has powers to "investigate, prosecute and bring to judgement crimes against the EU budget, such as fraud, corruption or serious cross-border VAT fraud." In the case of VAT offences, EPPO’s mandate is restricted to offences involving at least two Member States and more than EUR 10 million.

Turning to the Member States frameworks, one of the shortcomings identified by those we spoke to is the fact that **EU legislation has not always been fully transposed.** Thus, while all Member States have now transposed the PIF Directive it is not clear how fully they have done so. Ultimately, full transposition of the Directive by all Member States is essential to protect the EU’s financial interests as it harmonises the definitions of fraud, sanctions and limitation periods of criminal offences, and all these measures are needed to effectively tackle the problem. Furthermore, **the effectiveness of the EPPO is dependent on universal transposition of key measures** as the Commission stresses that “the Directive also lays the foundation for the material competence of the European Public Prosecutor’s Office (EPPO), which will investigate, prosecute and enforce these offences.” Beyond this, it has been argued that public procurement legislation as well as laws to combat corruption have not been completely transposed or are not being adequately enforced at the Member State level.
legislative gaps can be problematic for tackling organised crime as investigations and prosecutions occur mostly at the national level.64

Additionally, the research suggests that the definition of organised crime at the EU level is not harmonised across all Member States. It will significantly complicate the work of the EPPO if different Member States have differing definitions of issues the body has to investigate. If a case involving what the EPPO considers as organised crime is not defined as such in the Member State where the case is occurring, the EPPO cannot be involved in investigating the issue.

**Box 3.6: EU Definition of organised crime**

**Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime**

**Article 1: Definitions**

“For the purposes of this Framework Decision:

1. ‘Criminal organisation’ means a structured association, established over a period of time, of more than two persons acting in concert with a view to committing offences which are punishable by deprivation of liberty or a detention order of a maximum of at least four years or a more serious penalty, to obtain, directly or indirectly, a financial or other material benefit;

2. ‘Structured association’ means an association that is not randomly formed for the immediate commission of an offence, nor does it need to have formally defined roles for its members, continuity of its membership, or a developed structure.”

The definition of organised crime in the Italian criminal code has been suggested as a possible example of good practice.

**Box 3.7: Example - Defining organised crime in Italy**

**Mafia type criminal organisations**

**Art 416 bis Criminal Code**

“The association is of the mafia type when those who are part of it make use of the force of intimidation (3) of the associative bond and of the condition of subjection and silence that derives from it to commit crimes, to acquire directly or indirectly the management or in any case, the control of economic activities, concessions, authorizations, contracts and public services or to make unjust profits or advantages for oneself or for others, or in order to prevent or hinder the free exercise of voting or to procure votes for oneself or others in elections (4) (5).”

Another issue found particularly in cross-border asset recovery cases is that despite a number of legal instruments being introduced such as the Regulation on the Mutual Recognition of Freezing and Confiscation to enhance recovery, judicial cooperation is hampered by non-harmonised national rules and legal systems. Member States still faced obstacles in the execution of Mutual Legal Assistance requests and European Investigation Orders, in the identification and freezing of the proceeds of crime and in the recognition of confiscation orders issued by other Member States.65

Another potential shortcoming that has been reported by stakeholders lies in the overemphasis of ex-post timing when dealing with criminal investigation, i.e. after crime have been committed. In such cases it is difficult to collect evidence and effectively to prosecute offenders and recover funds.

---

64 Interviews
As a result, Latvian authorities, for example, in cooperation with the EPPO, have been working together to produce a manual with the most common typologies of fraudulent activities. This manual will also include also common suspicious activities so that programme authorities can recognise as fraud as well as allow law enforcement authorities to undertake criminal investigations at an early stage. Linked to this, another shortcoming reported by stakeholders is the very lengthy process of criminal investigation and prosecution, which can take several years, especially when the suspected crimes have an international dimension and investigations require assistance and inputs from other countries.

When it comes to the NAFS promoted by the Commission, none of the 13 EU Member States that have developed a NAFS have used the template provided by the Commission but their strategies include elements of it. One of the possible explanations for this situation is that some Member States had drafted their NAFS before 2014 when the Commission developed the guidelines and template.

These differences across Member States result in obstacles for efficient cooperation. Although the EU Strategy to tackle organised crime addresses the institutional structure within the EU to create a robust system with which to level up the EU’s efforts against organised crime, Member States will need to play their part to overcome current shortcomings. First, the strengthening of the legislative framework across Member States to establish compatible rules together with the streamlining and development of the instruments for law enforcement cooperation, for example through the proposed EU Police Cooperation Code, will be crucial to increase effectiveness in tackling organised crime across EU borders. Second, intelligence gathering at the national level needs to be improved to understand the nature and scale of criminal activities and the sectors at risk. This requires a more systematic collection of data and statistics based on common definitions (e.g. of ‘high-value targets’) so as to facilitate operational cooperation. This could be further strengthened by improving the interconnection of the relevant databases operated by EU Member States to speed up the exchange of information, and to increase coordination within and across Member States, particularly between administrative authorities and law enforcement bodies.

Similarly, the ECA found that in some countries there is a lack of cooperation and between administrative, judicial and law enforcement authorities as well as overlapping competences between these authorities. This is particularly the case when it comes to the exchange of data between customs and tax authorities, police, and prosecuting authorities which reduces the effectiveness of activities to fight against fraud. As elaborated below, the ECA highlights Belgium as having implemented good practice on cooperation between national authorities for tackling VAT fraud. Losses in fraud were reduced by 85% in two years by implementing a ‘joined up’ approach entailing better cooperation between authorities which allowed a focus on the disruption of organisers rather than targeting missing traders. The current European multidisciplinary platform against crime threats (EMAPCT) replicates at EU level the successful approach developed by the Belgium authorities.

Along the same line, and as third aspect to consider, the EU Strategy highlights the need to reinforce the Member State participation in EU wide networks, digital systems and data sharing platforms. The strategy mentions, among others, the e-Evidence Digital Exchange System (eEDES) to speed up...
the digitalisation of law enforcement activities and the judiciary, active participation in EMPACT to improve collective action against priority crime threats, and for all Member States to join the ON Network to reinforce its role in the international police cooperation in combating criminal groups.

Similarly, those we spoke to highlighted that the communication between the EU and the Member States should be improved. Part of this involves improving the sharing of data generated by the Member States with the Commission through IMS as well as enhancing operational cooperation. Interviewees also noted that in addition to integrating existing data tools at the national level with the EU level, these mechanisms also need to be integrated with Europol’s tools for crime investigation. In the case of Italy, for example, in order improve the reporting of cases of irregularities and fraud against the EU budget to OLAF in the context of EDES/IMS, national authorities have recently issued some guidelines for the national and regional authorities to help them address potentially critical elements in the communication of data and to standardise the reporting procedures.69

National enforcement capacity also needs to be developed as many Member States do not currently have the means to efficiently detect, investigate and prosecute organised crime. On the one hand, equipping national asset recovery offices with a more effective mandate, as proposed by the Commission’s forthcoming revision of the 2014 Confiscation Directive and of the 2007 Council Decision on Asset Recovery Offices, would contribute to improving the tracing and identification of illicit assets. On the other hand, developing tools and training in areas such as digital forensics, open-source intelligence and cryptocurrencies as well as the necessary skills in the field of criminal procedure, tactics and techniques for digital investigation, will be critical in levelling up Member State capabilities. The promotion of a culture of early financial investigation would further help build the capacity to tackle the financial dimension of organised crime.70

As noted earlier, there are also shortcomings in the transposition of the PIF Directive. The 2019 PiF report suggested that 18 EU Member States had fully transposed the PIF Directive, four Member States had only partially transposed it, three had not notified OLAF of their status, and one confirmed that they were not taking part in the activity.

---

**Box 3.8: Examples - Fighting fraud and organised crime in Member States**

- **Belgium**: Belgium has been highlighted as having implemented good practice in developing close cooperation between Belgian authorities to tackle VAT fraud. Losses in fraud were reduced by 85% in two years by implementing a ‘joined up’ approach and close cooperation between authorities which allowed a focus on the disruption of organisers rather than targeting missing traders. The approach implemented in 2001 entailed better circulation of interdepartmental information as well as within departments, a multidisciplinary non-operational support cell (called OCS) comprising both police and tax officers acting as central contact point for quick access to information, and the development of a dynamic risk analysis model for automated detection of fraud patterns. The approach also targeted first and foremost the organisers of fraudulent chains rather than the individual missing traders. As a result of these efforts, there was a significant drop in the VAT defrauded. In 2001, VAT fraud amounted to EUR 1.1 billion, in 2002 it was EUR 232 million and in 2003 the figure was EUR 159 million.71 The current European multidisciplinary platform against crime threats (EMPACT) replicates at EU level the successful approach developed by the Belgium authorities.

---

69 Guidelines on how to communicate to the European Commission irregularities and fraud against the European budget (link).
70 EU Strategy to tackle Organised Crime 2021-2025
• **Spain:** The National Anti-Fraud Coordination Service (SNCA) opened an online communication channel in 2017 in relation to projects or operations financed with EU funds in order to strengthen the collaboration with civil society and to formalize channels through which to allow for the reporting of irregularities to the relevant authorities. This aims to serve as additional means of identifying irregularities and to allow public authorities to carry out the corresponding investigations.\(^2\)

• **Finland:** a reporting channel specifically for suspected fraud in the European Structural and Investment Fund (ESIF) was implemented on the country’s website became operational in May 2019 with the aim of providing the general public with the opportunity for anonymous reporting of fraudulent actions relating to projects funded by ESIF. Since its launch, the channel has received a total of 4 reports concerning labour costs and conflicts of interest, out of which 3 were investigated as linked to specific projects. The Ministry of the Interior is responsible for recommending the necessary measures to be taken by the police.

• **Hungary:** Hungary has a unified IT system called FAIR (abbreviation for Database and Information System for Development Policy in Hungarian) for the management of EU funds. It manages all funding – those that are financed from ESA, ERDF, Cohesion Fund and European Maritime and Fisheries Fund (EMFF) - in an integrated system. Applicants fill in their applications through this system, funding contracts are registered here, payment are managed and checked through this system throughout the project period until the end of the project. The FAIR system is connected to the company register, the central database containing accounting reports, the database with the economic data of local governments, the land registry database, and the public debt and online account system of the tax authorities. When applicants apply for funding some of the data they enter is checked and filled in automatically. This allows the system to prevent ineligible entities from applying.

• **Latvia:** In Latvia, the investigative authorities did not start criminal proceedings in a number of cases identified by the managing authority and its delegated intermediate bodies. To analyse the reasons for these refusals and determine whether changes were required to working practices, the AFCOS set up an interinstitutional working group involving the authorities, the Ministry of Justice, the police and the State prosecution service. The working group now meets regularly to examine cases of suspected fraud in the implementation of Cohesion funding.

• **Latvia, Romania, and Hungary:** the use of Integrity Pacts in selected Member States, a pilot project supported by the European Commission and Transparency International, was highlighted by the European Court of Auditors in its 2019 Special Report 06 on fraud as good practice. The Integrity Pacts are an agreement in which the authority responsible for awarding a public contract and the economic operators bidding for the contract undertake to discourage corrupt practices and ensure transparency in the procurement process. The pacts also include a separate agreement engaging a civil society organisation (such as an NGO, a foundation or a local community-based organisation) to monitor all parties’ compliance with their commitments. The purpose of integrity pacts is to increase transparency, accountability and good governance in public contracting, enhance trust in public authorities and promote cost efficiency and savings through better procurement.

---

\(^2\) [https://www.igae.pap.hacienda.gob.es/sitios/igae-es/ES/snca/Paginas/ComunicacionSNCA.aspx](https://www.igae.pap.hacienda.gob.es/sitios/igae-es/ES/snca/Paginas/ComunicacionSNCA.aspx)
3.2.3 How many investigations and prosecutions have taken place and what proportion have been successful? How much EU funding has been retrieved? What have been the problems in seeking to retrieve EU funds?

Another shortcoming highlighted by the research is that fraud involving EU funds does not seem to be prioritized to the same extent as national level fraud. An indication of this is the fact that more than half of OLAF’s investigations are not followed up by national authorities and even less so when it comes to prosecutions. Another possible indication of this trend is in the differences between the Member States’ levels of involvement in the Eurojust’s case work. During the reference period, not all Member States have opened cases at Eurojust concerning PIF crimes and organised crime. Only 11 Member States did so and, among them, Bulgaria, France and Italy were the most active in that regard. However, all Member States without exception have been involved as requested parties in cross-border criminal cases concerning PIF crimes and organised crime. Germany, Poland and Romania were the most frequently requested Member States. It is possible that this situation may change as the latest Commission Anti-Fraud Strategy of 2019 intends to provide OLAF with a more centralised oversight role which inter alia will require Member States to justify reasons for not following up on OLAF recommendations.73

The study research suggests that efforts to tackle organised crime and fraud need to focus less on convictions and more on increasing the confiscation rate, which would act as a stronger deterrent to organised crime groups. One issue with the focus on convictions is that if successful, usually the conviction is limited to one individual who can be easily replaced within a larger network of organised crime. In this scenario, organised crime groups are not permanently thwarted and can continue to engage in illicit activity. At present, only 1.1% of criminal profits from EU fraud are currently confiscated across the EU. The argument is that if the confiscation rate could be raised to around 20% to 30% - similar to tax rates – organised crime groups would no longer consider such fraud to be profitable or worth the risk. It has been pointed out that confiscation has been made more difficult with the increasing use of cryptocurrencies. Interviewees note that the EU does not yet have an approach to tackle this issue.

Furthermore, when money arrives in the hands of organised crime, it is quickly moved out of the EU into offshore tax havens. According to interviews, it is estimated that around EUR 7.5 trillion held by organised crime groups is hidden in offshore tax havens. To tackle this issue, it has been suggested that the EU should adopt an approach similar to the extraterritorial approach adopted by the US authorities. Under this approach, the US has jurisdiction over dollar-denominated transactions regardless of the country in which the money laundering is occurring. This allows the government to exclude actors from the US economy and levy fines reaching US$100 million.

Member States have a legal obligation to recover the funds. That said, the money stolen from EU funds is not always retrievable as funding programmes sometimes close before any money can be recovered. There are two trends when it comes to recovering funds. On the one hand Member States appear to be improving in their recovery rate. For funds disbursed through DG REGIO for example, there was an 86% recovery rate for fraud for 2020.74 On the other hand, the Commission does not seem to be following up with Member States as often on identified issues of fraud.

73 European Commission. (2019). Commission Anti-Fraud Strategy: enhanced action to protect the EU budget
74 Kuhl, Dr. Lothar. (2020). Implementation of Effective Measures against Fraud and Illegal Activities in Cohesion Policies. EUCRIM
Table 3.1: Examples of prevention and detection actions

<table>
<thead>
<tr>
<th>Project lifecycle</th>
<th>Examples of prevention and detection actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application</strong></td>
<td>• Ensure transparency in the selection process</td>
</tr>
<tr>
<td></td>
<td>• Prevent conflict of interests within the Evaluation Committee</td>
</tr>
<tr>
<td></td>
<td>• Internal audit functions to conduct a secondary review of the Evaluation Committee decisions.</td>
</tr>
<tr>
<td></td>
<td>• Internal reporting mechanisms for fraud and corruption.</td>
</tr>
<tr>
<td><strong>Implementation</strong></td>
<td>• Ensure comprehensive audit trail and enhance on-the-spot checks</td>
</tr>
<tr>
<td></td>
<td>• Define standards of conduct for third parties</td>
</tr>
<tr>
<td></td>
<td>• Establish a sound and comprehensive e-procurement system</td>
</tr>
<tr>
<td></td>
<td>• Set standards for bidders for projects at-risk to fraud and corruption and/or with high investment value.</td>
</tr>
<tr>
<td><strong>Closure and evaluation</strong></td>
<td>• Ensure that auditors are subject to codes of conduct regarding project beneficiaries, contractors and third parties.</td>
</tr>
<tr>
<td></td>
<td>• Set standards for evaluators and experts, prevent conflicts of interest</td>
</tr>
<tr>
<td></td>
<td>• Verify and cross-check the information submitted for a project</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the Supreme Audit Institutions have the authority and capacity to provide external oversight of the ESI fund.</td>
</tr>
</tbody>
</table>

3.2.4 Have the Commission’s tools to detect and tackle fraud been effective? Would increased use of these tools by Member States lead to better outcomes?

The introduction of IT tools by the European Commission supports the shared responsibility of the Commission and the Member States to tackle and fight organised crime.

Although different in their legal status, Arachne is designed for voluntary use in the area of EU funding whereas the EDES is applicable to all aspects of the implementation of the EU budget under direct and indirect management, not shared management. Both tools contribute to detecting and preventing irregularities in the EU budget. Possibly given their quite recent introduction (Arachne is operational since 2013 and the EDES since 2016), the use of other complementary databases at the national level as well as the various EU-wide developments in parallel to combat organised crime, such as the introduction of a dedicated centralised authority to control financial transactions, might explain the limited information available on the results and effectiveness of Arachne and EDES as tools to detect and tackle fraud at national and EU levels.

Member States have also indicated that as they still use their own national systems for risk analysis, it is administratively burdensome to have to input data in both systems while not providing much added value for them. It has also been highlighted by Member States that it would be useful to be able to download Arachne data in an excel format to be able to more easily input this data into their own national systems. On the other hand, for Member States that find the data tool useful have highlighted that Arachne is only available for the Structural funds and cannot be used for funds as part of DG Agriculture for example. Authorities indicated there should be common tools for tackling all fraud rather than the system oriented towards specific funding programmes. This would allow authorities handling funds for migration policy and agricultural policy to make use of what the EU considers to be best practice. Integration of data tools could be across EU funds but also with national tax authorities. Other Member States have indicated that the data in Arachne can be inaccurate at times.
Previous studies and internal audits suggest that increasing awareness among authorities using these tools, the sharing of best practices, and training and workshops could increase their effectiveness. However, no data is available on the extent that this would be the case. The potential mandatory use of Arachne by all Member States, as suggested by the European Parliament for the 2021-27 period, could contribute to filling data gaps and thereby improving data management and quality of results of the tool, just as increased collaboration using the EDES would contribute to excluding unreliable entities from accessing EU funds in the first place. The direct impact the use of these tools is likely to have on detecting and tackling fraud and organised crime compared with the administrative burden they might entail remains uncertain.

Box 3.9: Examples – Member State fraud data tools

- **Germany**: established (by the 29 July 2017 Act) a Competition Register for Public Procurement. The system’s purpose is to prevent companies which have committed serious economic offences from benefiting from public procurement. The Competition Register allows authorities contracting services to check a single nationwide for companies that have committed relevant economic and competition law crimes. According to the Act, entities can be listed on the register for various reasons including bribery, human trafficking, formation of a criminal organisation, terrorist financing, money laundering, withholding of social security contributions, and tax evasion. Information for the registry can only be requested for specific reasons such as decisions awarding procurement contracts. An entity listed to be excluded is removed from the registry after a specified period of time (between 3 and 5 years). Companies listed can request to be removed if they demonstrate that they have addressed internal issues which had put the company on the list. Entities are notified before they are listed on the registry, allowing them to contest the decision. If this request is rejected, the entity can appeal to a regional court.75 76

- **Lithuania**: there is a new function within the Special Investigation Service (SST) the analytical anti-corruption intelligence department. The overall objective of the initiative is to strengthen data-driven corruption risk management by developing a data analytics model that provides a more effective and timely identification and analysis of corruption risks in order to prevent the manifestation of corruption-related offenses. It enables the analysis of a large amount of data available to the STT in a more efficient way and of a better quality, as well as various types of analyses, including visualization of a variety of data in different formats, that were so far not possible. Information on the project can be found here: https://ec.europa.eu/antifraud-knowledge-centre/library-good-practices-and-case-studies/good-practices/special-investigation-service-stt_en

- **Italy**: In 2019, the National Committee to combat fraud against the European Union (the Italian AFCOS) developed in partnership with the Ministry of Economy and Finance (MEF) an integrated National Anti-Fraud Platform (PIAF-IT). The platform was co-financed by the European Commission with resources from the "Hercule III" programme. PIAF-IT is a "business intelligence" platform that centralises, in a single database, data from different EU and national sources including for instance: the database of the MEF (BDU-IGRUE) containing information about the interventions supported by the EU structural funds; the database of the Ministry of Justice; data provided by the Court of Auditors and Chamber of Commerce. The platform also provides relevant information relating to beneficiaries of EU funds. The purpose is to make these data available to all national managing authorities and other competent bodies to strengthen their anti-fraud prevention capacity.77

75 https://www.bmwi.de/Redaktion/DE/Artikel/Wirtschaft/wettbewerbsregister.html
76 https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/23_10_2017_Wettbewerbsregister.html?nn=4548788
77 Department for European Policies - The "National Anti-Fraud Platform" starts in the field of European funding, high technology and information exchanges against wrongdoing (politicheeuropee.gov.it).
The Italian Court of Auditors has created another independent database, the SIDIF-CONOSCO (Community irregularities and fraud information system), to collect data about irregularities and errors in order to perform specific analyses related to its audit and jurisdictional functions. The database is a useful tool for monitoring public procurement audit errors and irregularities, as well as a means of performing analysis and identifying trends (Ibid). As the database contains information about the practices leading to errors, it can also serve as a risk assessment tool.

Other databases have been developed in specific sectors of the economy. For instance, in the agricultural sector, the national Paying Agency (AGEA) has set up a national database (“Registro Nazionale Debitori di AGEA Coordinamento”) that collects information about suspended requests for payment (through national and EU funds) because of suspected irregularities and fraud. Recently, AGEA and the Paying Agency for the Calabria Region (ARCEA) have also launched an anti-fraud system that aims to strengthen the anti-fraud prevention and coordination action in specific Regions with the highest number of suspended payments for irregularities by developing digital tools that will help detect fraudulent practices and corruption.

**Malta:** The Compliance and Investigations Directorate mentioned that the TNA tool has been very effective in detecting VAT fraud. The Anti-Fraud Unit assesses the involvement of the directors in other companies across the EU when vetting new VAT registration applications, and requests information on potential customers and suppliers of the applicant. The TNA allows the AFU to cross check these companies/traders, their risk level, and any potential involvement in fraud. This information is factored into the decision to approve or reject new registrations. The TNA tool also helps to detect potential VAT fraud involvement in post-VAT registration controls; it ranks traders according to their level of VAT fraud risk, which provides an early warning of potential criminal activity. The TNA also enables quicker and more efficient exchange of information and early detection of fraudsters within the Eurofisc framework, which Malta participates in. Malta has also used the Arachne IT Platform to combat fraud that affects EU Cohesion and Structural Funds in three formal inquiries. Interviewees said that the tool indeed helped in the detection of fraud, though provided no further detail.

**Denmark and Latvia:** The paucity and lack of data on organised crime is one of the major obstacles to implementing effective strategies at both the EU and national level. Some Member States have been pioneers in collecting data in specific areas where fraud might be an issue, such as is the case for Denmark. Denmark was the first Member State to develop a database for beneficial ownership. An NGO representative praised this Danish as a good practice and pointed out that Latvia was quick to follow suit and launched its own database. Latvia was also described by the same NGO as a Member State exhibiting good practice in terms of data on public procurement, an area where organised crime is known to operate.

**Arachne**

The Arachne Risk Scoring Tool, developed by the European Commission and operational since 2013, is a voluntary preventive detection tool used by some Member States in the area of the Structural Funds (European Social Funds and the European Regional Development Fund). As an integrated IT tool for data mining and data enrichment through both internal and external information, it provides data on projects implemented under the Structural Funds in form of a comprehensive database. In order to identify exposure to risks of fraud, conflicts of interests, double financing, corruption or other irregularities of projects, beneficiaries and contracts and contractors, the system alerts the Managing...
Authorities (MAs) where the data suggests there could be risks of fraud. As a result, the authorities can focus their administrative controls on the projects considered at risk, run the necessary verifications so as to prevent, detect and correct irregularities or fraud, and notify OLAF via the Irregularity Management System (IMS) database. Arachne is provided free of charge to MAs.

By offering the development and the implementation of Arachne to all Member States, the European Commission aimed to contribute to a more systematic data collection and enrichment effort at national level and to support the effective detection of illegal practices. Especially in the context of decentralized Member States’ administrative responsibilities for the implementation of Cohesion policies, this was intended as a valuable contribution towards stepping up the efforts against irregular practices in a coordinated and harmonised manner. However, according to Article 125(4) of Regulation 1303/2013, the responsibility for implementing anti-fraud efforts ultimately lies with Member States, which must “put in place effective and proportionate anti-fraud measures”, be it by implementing Arachne or making use of other domestic systems.

By September 2019, 20 Member States used Arachne, out of which 16 had integrated it into their management and verification processes for at least one operational programme. According to the Commission’s figures, Member States used Arachne for 165 operational programmes in 2018, which accounts for 54% of all EU Cohesion funding for 2014-2020, with the exclusion of the European Territorial Co-operation objective of the European Regional Development Fund. Among the most active users were Slovakia, Czechia and Bulgaria, as well as France, Italy, Latvia and Romania. At the same time, other Member States abstained from using it: Austria, Germany, Sweden, Finland and Denmark had not implemented the tool whereas Poland and Cyprus were still undecided. The reasons for this situation include stricter national rules on data confidentiality and protection, for example in Germany, and plans to develop alternative national systems, as in Poland. Arachne is often used by authorities in combination with other IT tools, most frequently national IT tools and databases with a narrower geographic scope. In those countries where Arachne is not used, national and regional IT systems or other similar tools and databases are in place, which offer similar functionalities.

A study by the European Policies Research Centre assessed the perceived effectiveness of anti-fraud measures in Cohesion Policy by surveying MAs. Among the fraud detection measures, the Arachne risk-scoring tool was perceived to be the least effective (5.4 points out of 10); those with the highest effectiveness rating were: on-the-spot checks and audit (9.0/10), internal fraud reporting mechanisms (8.4/10) and fraud risk assessment on project applicants/beneficiaries (7.7/10). These findings suggest very mixed views amongst MAs in relation to the benefits of implementing Arachne. Nevertheless, a study commissioned by DG REGIO in 2018 established that, although about two-thirds of the MAs interviewed did not use Arachne, the majority of those that had used it saw it as being effective with regard to the assessment of potential conflicts of interest and identifying red flags, given the otherwise...
resource-intensive nature of the task. Only some MAs used its full functionalities, with half of them reporting the use of functionalities for the identification of conflict of interest or fraud ‘red flags’.

No detailed data is yet publicly available assessing how effective this tool has been in detecting and tackling fraud neither at EU nor at national level, and no evidence has been identified in terms of the impact of using the tool in increased prevention of fraud and organised crime towards the EU budget. This might be due to the recent implementation of Arachne by some Member States, as the tool can help MAs to document increased effectiveness and efficiency in managing verifications and risk assessments over time; another factor could be the uneven implementation within individual Member States themselves, especially in cases where implementation responsibilities are delegated to intermediate bodies at the national and regional levels, as in France and Austria.

Besides the use of national databases complementing Arachne, further EU-wide developments in the fight against corruption such as the obligation for countries to introduce a dedicated centralised authority to control financial transactions (i.e. the Fourth European Money Laundering Directive) as well as additional efforts by some countries in recent years to level up their efforts against organised crime (e.g. in Slovakia), might make it rather challenging to establish a direct causal relation between the use of Arachne and a higher detection, prevention and tracking of organised crime activities. It has been pointed out in interviews that Arachne’s access to data required to prevent fraud is at times limited due to national legal constraints. It is, for example, not possible to gather information on family members or spouses of beneficiaries though this is often a channel through which fraud occurs.

However, one conclusion is evident: the success of Arachne relies to a large extent on the input of data by MAs for calculating risk indicators as well as on the capacity of data systems to communicate with each other. As such, an increasing uptake of Arachne for all programmes and Member States is likely to lead to more complete information being included in the database and thereby a further increase its quality and effectiveness. As indicted in the Arachne Charter, in cases of recurring identified risks, control systems could be reinforced so as to serve as a preventive measure in future, also leading to an increasingly effective system.

The interoperability of Arachne with other databases used in relation with the European Structural and Investment Funds at a national level, such as the Information Technology Management System, the Irregularity Management System, and the Early Detection and Exclusion System, as well as complementary information from company registers and procurement databases, would be crucial to increasing the impact of IT tools in detecting fraud. One interviewee highlighted the fact that a way to improve the usefulness of the data is to make it public and fully integrated with the national systems for collecting data as this will remove the administrative burden of having to reinsert the data into Arachne, thereby streamlining the process.

It has been pointed out that because it is voluntary, Arachne, is not used by some Member States and is used to only a limited extent by others. Certain challenges continue to act as obstacles for an increased uptake of Arachne, as identified by Member state authorities in studies carried out in recent

---

89 [https://ec.europa.eu/sfc/sites/default/files/study-_implem_article125_en-final.pdf](https://ec.europa.eu/sfc/sites/default/files/study-_implem_article125_en-final.pdf)
91 Interview
92 [https://www.oecd-ilibrary.org/sites/d4c5cea4-en/index.html?itemid=/content/component/d4c5cea4-en](https://www.oecd-ilibrary.org/sites/d4c5cea4-en/index.html?itemid=/content/component/d4c5cea4-en)
95 [https://www.oecd-ilibrary.org/sites/d4c5cea4-en/index.html?itemid=/content/component/d4c5cea4-en](https://www.oecd-ilibrary.org/sites/d4c5cea4-en/index.html?itemid=/content/component/d4c5cea4-en)
96 Interview
years. These include legislative barriers, in the form of compliance with national data protection laws and the uncertainty around the legal status of the tool for those countries that decide to make use of it, for example in terms of consequences of a potential late provision of data, stipulated in the Arachne Charter to take place every three months. Lack of functionality and risk indicators not being relevant for some - often smaller - types of projects were reported as some of the concerns hindering greater implementation across the EU, together with the high number of false positives for potential conflicts of interest, fear for additional audit and disproportionate administrative burden.

Improving the use of data analytics tools and techniques, including risk-scoring tools like Arachne as well as strengthening the use of national databases would contribute to a **more robust data-driven approach to fraud and corruption risk management**. Going one step further and making the use of Arachne mandatory for all EU Member States, as suggested by the European Parliament, would contribute to an increasing streamlining of data collection and analysis in the context of organised crime and increase the effectiveness and quality of the tools available.

**Box 3.10: Transaction Network Analysis (TNA)**

- The Transaction Network Analysis was developed by the Commission at the request of the Member States and was placed at the disposal and use of Eurofisc, a network of anti-fraud tax experts from Member States. Each Member State runs their own risk management system based on information from the national VIES databases. The TNA performs automated selection of information available in the VIES system based off of risk indicators which allows for detection of fraud patterns and chains involving several entities. In 2020, Eurofisc progressively increased the use of the Transaction Network Analysis (TNA) system, to exchange, share and jointly analyse targeted information on VAT fraud. During this year, which was the first full year of TNA operations, Eurofisc transitioned from the use of legacy tools to this new, advanced system for data exchange and analysis.

- Eurofisc has reported that the introduction of the tool has been very beneficial. Eurofisc officials highlight that by using TNA the Member State’s tax administrations can detect and react much quicker to cross-border VAT fraud. In addition, TNA helps Member States to produce statistics more efficiently, thereby better demonstrating the positive impact and potential of Eurofisc. Only in the first year of full operation of the TNA in 2020, Eurofisc monitored 1,800 potential fraudsters involved in EUR 3.3 billion worth of fraudulent transactions and flagged another EUR 2 billion worth of suspicious transactions.

**Early Detection and Exclusion System (EDES)**

**EDES is a mechanism to protect the EU’s financial interests against unreliable economic operators and fraudsters and to ensure sound financial management.** Besides allowing for early detection of persons and entities representing risks to the EU’s financial interests, it allows for the exclusion of unreliable entities from obtaining EU funds and provides for a broad range of sanctionable practices with financial penalties.

Since 2016, EDES applies to all contracts, grant agreements, financial instruments, prizes, remunerated experts and for the implementation of the EU budget under direct and indirect management (not to shared management, as for the latter irregularities are reported in IMS as separate database).

---


includes operators which are in bankruptcy, have perpetrated fraud or corruption in the past, have been identified as participating in organised crime or have committed grave professional misconduct (Financial Regulation, Article 136(1)).

The introduction of an operator into the EDES is done at the request of an authorising officer of an EU institution and after review and the recommendation to do so by an inter-institutional panel presided over by a high-level independent chair (Financial Regulation, Article 143). It is the panel which is responsible for issuing recommendations for exclusion and/or financial penalties as well as the publication of serious cases in the public EDES database where applicable. This central assessment is considered to represent “a significant improvement in the application of rules on administrative sanctions with respect to fundamental rights, independence and transparency”. Following the recommendation by the EDES panel, the authority to decide on the proposed administrative sanction of a given economic operator lies with the requesting authorising officers.

The increase in admissible cases for review by the panel in the last years suggests increasing awareness of the system among EU Member States as well as increasing collaboration with OLAF. In 2019, 19 admissible referrals were made to the panel as compared to six admissible cases in 2018. A total of 83 cases have been admitted by the panel since its foundation, out of which it has issued 43 recommendations, 5 of which were recommendation of non-exclusion. As a result, there have so far been 33 exclusion decisions by authorising officers. Cases of exclusion from EU funds due to fraud specifically using the EDES are limited and quite recent. The two first recommendations by the panel of exclusions on the grounds of fraud took place in 2018, following the revision of the 2015 Financial Regulation and the introduction of the preliminary classification in law for fraud. Fraud could not be used on facts committed before 2016, in observance of the general principle of legal certainty.

Limited information is available on the overall effectiveness of the EDES in the detecting and tackling of fraud. An audit by the Internal Audit Service of the European Commission in 2019 concluded that the EDES system is well integrated in local IT systems, thereby allowing for early detection or exclusion in EDES of economic operators receiving funds from Horizon 2020 programmes. It also recognised the role of the EDES Panel as having the necessary expertise and experience to undertake its tasks effectively and highlighted the use of best practices from the World Bank Suspension and Debarment system as one of its ‘undeniable strengths’. This may be referring to the Sanctions for Fraud and Corruption, which include practices such as proportionality (the sanction fits the nature and scope of the Sanctionable act), independence of judgment (among the members of the Sanctions Board), and transparency with both recipients of sanctions and the wider public.
The study research suggests that **EDES can begin excluding beneficiaries before judicial proceedings against such actors have been finalised**, thereby allowing for a quick response, which is necessary in tackling fraud. On the other hand, the Commission’s decentralised system means only national authorities can start the exclusion of these operators. Additionally, there is scope for improvement, for example increasing awareness of EDES and the potential analysis of access to EDES database in relation to shared management funds by Member States’ authorities.\(^{111}\) Additional guidance in the form of a corporate guide, improving the follow-up of OLAF reports and recommendations, as well as identifying steps to avoid delays in the EDES Panel procedures, were additional recommendations. One issue highlighted by an interviewee is that the functioning of EDES is burdened by legal and administrative requirements which prevents efficient and early detection of problematic beneficiaries. An example of this is the right of appeal, which in the EU can be initiated at several levels including the European Court of Justice as well as the EDES Panel. This was contrasted by an interviewee with the situation at the World Bank which only has one appeal process with two stages: the Access to Information Committee, and subsequently the Access to Information Appeals Board.\(^{112}\)

In our research, some Member State authorities have indicated that they find the EDES system to be inflexible and hard to use. As an example, they have indicated that after having flagged an entity for exclusion, it is not automatically registered for exclusion in the system and can instead take months and sometimes a year for this to occur. This creates a delay when it comes to enforcement at the Member State level. It can sometimes be the case that when a decision has been made to exclude an entity for 2-3 years, it can take half of their sentence for them to be included on the EDES registry. Additionally, some Member States have noted that EDES does not include key identifier information such as the tax number of the companies listed. Considering that the number of organisations listed in EDES is limited for each country, local authorities have indicated that it would be useful to receive notifications when new national subjects have been entered into the database. Some Member States have also indicated that they would find it useful to have detailed information for the reasons why an entity has been registered on the system for exclusion (as is the case in the German exclusion registry detailed in a box above). Some authorities have created their own database which they manage in parallel due to the difficulties.

These findings suggest an expected increase in effectiveness of EDES once the recommended actions are put in place. For example, the Commission has already undertaken significant efforts to raise awareness of the EDES among Commission services and EU delegations. Furthermore, the Commission has developed a targeted communication strategy and highlighted EDES as “an important tool for sanctioning fraud and serious misconducts” at international events.\(^{113}\) 2019 was the first full year in which the EDES Panel functioned under the revised Financial Regulation, which is considered to have contributed to significant improvements to the system. As an example, new grounds of exclusion were introduced and the provisions relating to the system were streamlined and clarified. Given the very recent introduction of these and other improvements, additional time will be needed for their results to become fully apparent. For the time being, no evaluations nor relevant studies looking into the effectiveness of EDES, either before nor after the revised Financial Regulation, have been identified, and thus the potential improved effectiveness resulting from an increased use by Member States remains uncertain.

---

111 http://europeanmemoranda.cabinetoffice.gov.uk/files/2019/10/st13091-ad03.en19_.pdf
113 http://europeanmemoranda.cabinetoffice.gov.uk/files/2019/10/st13091-ad03.en19_.pdf
3.3 Conclusions – EU and Member State approaches to the problem

The PIF Directive and the EU’s Strategy on Organised Crime (2021-25) represent significant steps towards forging a common approach to tackling the problem of organised crime fraud in relation to EU finances. That said, while all Member States have transposed the PIF Directive, there are varying degrees of implementation. Furthermore, while the Commission has encouraged Member States to develop National Anti-Fraud Strategy (NAFS), so far progress is limited.

The capacity of national authorities to address the challenge of organised crime in relation to the EU finances varies considerably across the EU Member States and while some have well-developed strategies, resources and mandates, others do not. This also creates challenges and obstacles for efficient cooperation. Differences between Member States in terms of reporting on fraud and irregularities arise because of differences in national systems to counter fraud as well as non-harmonised reporting systems. Similarly, the EU level tools to detect and prevent fraud are not used by all Member States or are not used extensively by some others. An additional complication is that there is no distinction in some Member States between national financial crimes and EU financial crimes. This study suggests that a key priority is to develop a common approach to estimating the level of fraud affecting the EU finances and in relation to the measures taken by Member States to tackle the problem.
4 MODELLING THE ESTIMATES OF EU EXPENDITURE-RELATED FRAUD

The second part of the methodology for this study provides quantitative estimates of the impact of organised crime on EU finances based on a model developed by one of our external experts (Dr Mihály Fazekas, Scientific Director, the Transparency Institute and Assistant Professor, Central European University). More specifically, it seeks to estimate the costs of organized crime infiltration risks for the EU budget in the area of government procurement.

As noted earlier in Section 2, the extent to which EU expenditure in Member States is subject to the misappropriation of funds, whether by organised crime or other perpetrators, has proved especially difficult to quantify. Existing figures, by their own admission, tend to be conservative and understate the scale of the problem. We have sought to address this shortcoming by undertaking a modelling exercise to estimate the costs of organized crime infiltration risks for the EU budget in the area of government procurement. The research utilizes a unique EU-wide dataset of public procurement and uses the predicted probabilities in regression models explaining prices of awarded contracts.

4.1 Introduction - Problem of Organised Crime and Public Procurement

It is well established that organised crime facilitates political corruption in many countries, including the EU Member States (Gounev and Ruggiero 2012). Public procurement infiltration serves as an important channel for maintaining influence in the legitimate economy for organised crime groups (Ravenda et al. 2020, Caneppele and Martocchia 2014). The presence of organised crime groups in public procurement leads to significant costs for public budgets due to overly expensive and inefficient spending, as well as a lower quality of the purchased goods and services.

Organised crime can infiltrate public procurement at different stages in the procurement process. To reduce competition and unfair advantages in access to contracts for certain firms, organised crime groups might engage in different forms of collusion, as well as try to influence officials and politicians to facilitate non-competitive tendering procedures. They might also use the political connections to secure more favourable contractual terms, and thus increase profits. Finally, such groups are interested in influencing enforcement mechanisms to avoid the detection and deterrence of fraud and collusion.

The European Structural and Investment funds constitute a large part of EU spending - more than EUR 450 billion was allocated for the programming period of 2014-20. Organised crime infiltration constitutes a particular risk of corruption in EU funds allocation given that a significant part of investments are directed to areas such as construction, energy, and environmental protection where there is thought to be greater scope for organised crime infiltration.

4.2 Modelling Approach to Estimating Organised Crime Fraud

The analysis builds on a recently published DG HOME study on the risks of organised crime infiltration in legitimate businesses. The modelling exercise draws on several sources.

The first one is the micro-level dataset of public procurement in the EU that was collected from the Tenders Electronic Daily portal by the Government Transparency Institute as a part of the DIGIWHIST project. It contains the dependent and control variables that are used in the analysis and covers the

---

The period from 2011 to 2020. Multiple filters have been applied to the dataset to obtain the relevant sample for the analysis. First, only contracts awarded by the local procuring entities were analysed. This sample restriction was applied because the initial organised crime infiltration model was developed using public procurement data in Italian municipalities and extrapolation to other types of organisations such as central government entities is not warranted. Second, we have restricted the sample to contracts that co-financed by the EU.

The second source is a predictive model of organised crime infiltration risk that we have developed for a recently published DG HOME study. This model learns from proven cases of mafia infiltration in Italy and extrapolates the identified risk factors to the whole EU. Extrapolation is supported by both theoretical arguments around how organised crime groups use corruption in public procurement and also empirical tests which show that the predicted public procurement organised crime scores overlap with other, well-established indicators of infiltration.

The database of public procurement tenders in Italy for the period 2008-2014. To develop this predictive model of organised crime influence, two Italian administrative datasets have been combined. The first dataset contains the information on the dates of dissolutions of local governments in Italy due to organised crime infiltration. The second dataset, maintained from the ANAC, contains data on Italian public procurement contracts with a reserve price of more than EUR 150,000 for the period 2008-2014. The matched dataset provides information on the key contract-level and regional variables that served as features of the predictive model, as well as a binary indicator of the organised crime infiltration of contracts. Annex C provides a description of the data sources, data matching and modelling methodology.

Estimating the risk of organised crime infiltration in public procurement builds on the methodology developed by Fazekas et al (2020) and Hulme et al (2021, Section 3.3). We developed traditional regression models as well as tree-based machine learning models using our unique dataset of public procurement tenders with the binary indicator of mafia presence. Thus, the models for predicting organised crime infiltration probability at the contract level were based on a set of proven cases for which it is known whether infiltration took place or not based on official data. Dissolving a municipal administration in Italy due to mafia infiltration very likely means that the awarded contracts before dissolution were controlled by mafia-like groups. While the contracts awarded after dissolving the municipality (i.e. when the central government took over local administration) means that contracts are very likely to be free of mafia-like groups’ influence. We were able to define the infiltration status of the contracts by exploiting the dates of dissolutions of local governments that were proven to be infiltrated by the mafia. In particular, a contract was marked as influenced by organised crime if it was awarded in a municipality which was dissolved 3 years before dissolution. Alternatively, a contract was marked as not influenced by organised crime if it was awarded in the 3 years period after the dissolution.

Such a unique dataset of the marked cases of organised crime infiltration at the level of procurement contracts has allowed us to develop a set of models capturing the most essential features of what organized crime control looks like in public procurement. Crucially for extrapolating to the EU as a whole, these models capture generic features of contracts such as number of bidders or concentration of spending which signal any type of organised crime presence or institutionalized forms of political corruption, not only mafia groups. Hence, while our models learn from mafia-like groups behaviour, the patterns identified apply more broadly to organised crime groups across Europe.

---

115 Logistic regression, Boosting and Random Forest.
As there are only a few studies exploring the effects of indicators of organised crime infiltration in public procurement, the analysis draws on the existing literature on the tendering corruption risk (Fazekas et al, 2016) to select the set of relevant features for developing the predictive models. As organized crime groups are likely to utilize various forms of corruption in their operations, all of the tested models included significant ‘red flags’ variables such as number of bids, procedure type used, or share of supplier in buyer’s annual spending in order to capture restricted competition that is expected to occur due to organised crime infiltration in public procurement. We have also used the set of contract-specific (e.g., contract value, procedure type, market) and region-level variables (population, area, binary indicator of whether a region is located in a mountain or coastal area). The set of predictors was restricted in order to allow for EU-wide extrapolation using the EU-wide public procurement data (i.e. all variables only available in the Italian public procurement dataset but not in Tenders Electronic Daily were removed from the analysis). The full list of indicators used in the model is provided in Annex N (Table A1).

Based on the percent correctly classified contracts on the test dataset with 70% of the sample, a Random Forest classifier was selected as the best performing model and used it to make the EU-wide prediction of organised crime infiltration risk score using micro-level dataset of public procurement in the EU. The details of the models development and selection are provided in Annex B.

The organised crime infiltration probability score was validated both on Italian and EU-wide samples. For the Italian data, we validated the indicator using Transcrime’s Italian province-level mafia index. Specifically, we found positive and significant correlation between the predicted OC infiltration risk score and the mafia index. In turn, for validation of the EU-wide extrapolation, we aggregated our predicted OC infiltration risk score from the contract to country level. Then the expected positive correlation between our predicted country-level risks and other established organised crime indicators such as companies’ links to blacklisted jurisdictions offer support for the wider applicability of our model.

Figure 4.1: Predicted organised crime infiltration probabilities averaged by European NUTS3 regions, based on the sample of EU-funded contracts awarded by municipalities

---

Note: countries with less than 300 contracts were removed from the sample.

The map in Figure 4.1 represents the results of the EU-wide extrapolation using the outlined model. In particular, it shows organised crime infiltration probabilities in EU-funded contracts awarded by municipalities, using data from the EU-wide TED procurement data source. Only countries with more than 300 contracts in the 2011-2020 period were considered. The regions filled with white colour are those for which the extrapolation was not possible due to low level of observations.

As can be seen from the map (Figure 4.1), the model predicted higher than average probabilities of organised crime infiltration for regions in the Mediterranean and Eastern Europe. For example, southern Spain and Italy received high scores, along with Eastern Slovakia and Hungary, as well as swathes of Romania and Bulgaria. Nevertheless, selected regions in otherwise high integrity countries such as France have also seen a high predicted organised crime infiltration risk.

4.3 Conclusions – Modelling Estimates of EU Expenditure Related Fraud

Based on the modelling exercise focusing on a sample of contracts, a range of scenarios have been developed:

- **Lower estimate** – Our lower estimate is based on lowering the share of medium to high organised crime infiltration risks by 50%. This scenario is estimated to save approximately 2.7% of total spending, in the sample of local procuring entities. This corresponds to about EUR 536 million of potential savings for the period of 2011-20 for the sample or some EUR 1.9 billion if scaled up to include all EU-funded public procurement.

- **Higher estimate** – Our higher estimate is based on eliminating all medium to high organised crime infiltration risks. This scenario leads to potential savings of about 3.6% of total spending, in the sample of local procuring entities, corresponding to approximately EUR 689 million over the 2011-20 period or EUR 2.6 billion if scaled up.

These absolute savings values most likely underestimate the true value of savings because the sample of procurement contracts recorded in Tenders Electronic Daily (TED) with sufficient data quality has been shown to omit considerable amounts of EU funded procurement spending (e.g. contracts falling below the EU Directive thresholds). Applying the conservative scenario to all relevant EU Cohesion Funds (allocated spending in the latest 2014-20 programming period was EUR 72.6 billion117) yields a total savings of about EUR 1.9 billion. Similarly, the higher estimate scenario is applied to all ESIF Funds, there is a total potential saving amounting to about EUR 2.6 billion. It should be noted that these scaled up savings estimates depend on a number of assumptions such as the same price sensitivity of procurement to organised crime infiltration risks across all types of ESIF spending.

Contracts in markets such as infrastructure, software packages and information systems, machinery, and recreational, cultural and sporting services, are more likely to be influenced by organised crime fraud according to the results of our modelling. In terms of contract value, middle-sized contracts are predicted to have a higher infiltration score on average. Specifically, contracts from the middle of the distribution (i.e. second quartile) are predicted to have a mean organised crime infiltration score of around 0.3, while for the rest of the sample the average predicted OC probability is notably lower, at around 0.2-0.25.

**Limitations of the Analysis**

While the methodology is highly sophisticated and rests on large-scale datasets, it nevertheless faces a number of limitations which future research may be able to alleviate.


118 The average OC infiltration score for the contracts in these markets is higher than 0.3.
Given data restrictions, the model of organised crime infiltration prediction was developed using the sample of public procurement contracts awarded by Italian municipalities. The adopted methodologies capture commonly used techniques for restricting competition and corruptly organising procurement tenders and implementing contracts. Our extrapolations for the whole of Europe rest on the applicability of these indicators outside of Italy. While there is ample evidence that the identified risk factors and the underlying corrupt behaviours occur throughout Europe (Fazekas et al, 2016), our models could not account for possible national and regional features of OC influence in public procurement.

Moreover, price modelling also includes data limitations. The predicted absolute savings values most likely underestimate the true value of savings because the sample of procurement contracts recorded in TED with sufficient data quality has been shown to omit a considerable amount of EU funded procurement spending (e.g. contracts falling below the EU Directive thresholds). Savings figures were also calculated using contract values at the time of contract award; however, a range of studies have shown that contract values and implementation quality can considerably change during the contract execution phase. Such changes are most likely to occur where corruption took place, hence potentially pushing the cost of OC infiltration further up. Such costs and hence potential savings would need to be investigated further once the corresponding data becomes widely available.
CONCLUSIONS & RECOMMENDATIONS

In this final section we summarise the overall conclusions of the study and then present more specific conclusions and recommendations with regard to actions that could be taken at the EU and Member States’ levels to strengthen efforts to reduce the impact of organised crime on the EU’s finances.

5.1 Overall Conclusions

Fraud perpetrated by organised crime against the EU’s finances is a serious problem that significantly reduces the capacity of the EU to address the many challenges that Europe faces. It has even been suggested that the losses to the EU finances, if prevented or recouped, would be sufficient to cover the public health costs associated with the COVID-19 pandemic.

Although thought to be on a large scale, the extent to which organized crime is benefiting illegally from the EU’s finances is difficult to estimate with great precision. In part this is because of definitional issues, specifically the fact that there are differing definitions of organised crime, but also because by its very nature there is likely to be a large ‘hidden’ element of undetected fraud against the EU finances. Our best estimate based on the research and the calculations in Section 4 is that fraud perpetrated by organised crime is likely to amount to some EUR 50 billion expenditure and revenue p.a. Assuming a uniform VAT call rate of 0.3% this means that the EU budget is likely to incur losses of EUR 150 million of revenues that can be attributed to organised crime groups together with a further EUR 2.0 billion to EUR 2.7 billion p.a. on the expenditure side. This amounts to between 1% and 2% of the EU’s budget of EUR 165.8 billion for 2020 budget.

On the revenue side, organized crime activities relate to VAT fraud, the most common type, and to customs fraud. ‘Missing trader fraud’ is thought to account for most of this and because of the complexity of the schemes is likely to be almost exclusively perpetrated by organised crime groups. When it comes to MTIC fraud, it is estimated that between EUR 40 billion to EUR 60 billion is lost per annum to organised crime groups.119 Another estimate put the size of VAT fraud at € 50 billion p.a., one of several contributing factors to the VAT gap of nearly € 160 billion p.a. estimated by the Commission in 2014.120 Another indication, from the UK, is that VAT fraud had amounted to some EUR 2 billion per annum in the UK. A significant factor is the growing proportion of VAT fraud associated with eCommerce which is now thought to account for somewhere between 8-12% of the VAT ‘gap’.121

In relation to EU expenditure, fraud tends to be perpetrated to a greater extent than on the revenue side by both individuals and businesses as well as organized crime groups. On the other hand, while the picture is clearer on the extent to which organised crime is involved in defrauding EU revenues, authorities are unclear as to how much fraud of EU expenditures is committed by organised crime. OLAF suggests in its last PIF annual report (2019) that Member States identified 11,726 irregularities (fraudulent and non-fraudulent) to the Commission amounting in 2019 to EUR 1.6 billion (a decline of 34% compared to 2018). Not all these irregularities are, however, accounted for by fraud. Specifically in relation to the cohesion and fisheries funds, OLAF estimates that some EUR 366 million of the EUR 1.6 billion could have been the subject of fraudulent activities. Our own estimates suggest that the figure could be much higher than this. Several reports highlight the danger that organised crime groups will take advantage of the support and recovery schemes launched to help the EU recover from the Covid-

---

19 pandemic. As noted above, our own quantitative modelling suggests a higher figure for fraud on the expenditure side.

**Overall, it is clear that a lot more needs to be done to effectively tackle the problem of fraud against the EU finances, both by individual entities as well as organised crime.** Whilst key elements of the legal framework and other anti-fraud measures are in place at the EU level - including the PIF Directive, the EU’s 2021-25 strategy to combat organised crime and the EPPO - there needs to be a step-change at the Member State level in efforts to deal with the problem.

### 5.2 Specific Conclusions and Recommendations

Below we set out more specific conclusions and recommendations, firstly at the EU level and then for Member States.

#### 5.2.1 EU level

The PIF Directive and the EU’s Strategy on Organised Crime (2021-25) represent **significant steps towards forging a common approach to tackling the problem of organised crime fraud in relation to EU finances**. That said, while all Member States have transposed the PIF Directive, it is possible that there are varying degrees of implementation. Furthermore, while the Commission has encouraged Member States to develop National Anti-Fraud Strategy (NAFS), so far progress is limited.

**Definitional issues**

At present, there are differing definitions of organised crime across EU Member States which makes it more difficult to coordinate measures to combat fraud against the EU’s finances. The lack of harmonisation across Member States is likely to make it more difficult for the EPPO to carry out its role, especially in transnational cases of suspected fraud where organised crime is involved. Moreover, if the EPPO believes that an organised crime group is behind a crime affecting the financial interests of the European Union, but the Member State involved does not qualify the conduct as organised crime because of their national legal definition of organised crime, the EPPO cannot launch its investigations.

**Recommendation 1: Harmonise national definitions of organised crime to ensure EPPO has competencies over all cross-border cases.** Harmonising definitions would make it easier for the EPPO as well as Member States to investigate and prosecute cross-border cases of involving organised crime’s attempts to defraud EU financial interests. In this regard, Member States should follow the definition of organised crime outlined in the Council Framework Decision 2008/841. This would also help in obtaining a clearer picture on the extent to which organised crime is involved in defrauding EU’s financial interests across Member States as it would allow for cross-country comparisons on a more consistent basis.

**Use of EU Tools to combat fraud**

At present, the EU data systems such as EDES and Arachne are not being used to their full potential as tools to help combat fraud against the EU’s finances. A total of 20 Member States use Arachne and 16 of them have integrated the system into their own management and verification system for at least one EU programme. At present, EU data tools such as EDES and Arachne are not mandatory for Member States and not all of them make use of these tools. Other Member States make

---

use of the tools but only to a limited extent. Feedback from the national authorities indicates that many find these tools cumbersome, partly because they are not integrated, and do not see the added value of using them, particularly when some Member States have their own well-developed systems.

**Member State authorities who do not use Arachne have cited numerous reasons for this situation.** Some member states have indicated that they do not use EDES as the data is entered too late to be of use. For instance, it was mentioned that even if a judgement is enforced which prevents an organisation from obtaining EU funding it does not mean that they are automatically added to the EDES database, which creates a delay in enforcement at the Member State level. Moreover, EDES sometimes does not include all the necessary identifier information about an organisation such as the tax number of companies (the inclusion of the tax number would make the identification of individuals and companies easier). Furthermore, as the number of organisations listed in EDES is very limited (in some countries only 2 or 3 entries).

Some of those consulted for the study argue that EDES is burdened by legal and administrative requirements which prevent efficient and early detection of possible fraud. One indication of this is in relation to the right of appeal, which in the EU can be initiated at several levels, such as the European Court of Justice and the EDES Panel. A multi-stage system provides easier access but it is also more complex and time-consuming. This contrasts with the situation at the World Bank which only has one appeal process with two stages (the Access to Information Committee, and subsequently the Access to Information Appeals Board).

Apart from further developing the EU anti-fraud tools feedback from the research suggests that the different data collection and risk analysis tools available in the EU should be better integrated. This includes integrating the Commission’s tools to combat fraud with Europol’s tools for crime investigation. Additionally, it has been suggested by some of the national authorities that find Arachne useful, that the tool should be available to all national agencies managing EU finances as well as administrative and criminal investigation authorities, not just managing authorities involved in the Structural Funds.

**Recommendation 2:** The Commission should support and encourage Member States to use both EDES and Arachne to tackle fraud and organised crime. Increased use by the EU Member States would improve the utility of the EU tools. With an aim to have all Member States adopt these EU tools, minimum requirements should be established for each of the Member States’ data collection and risk analysis systems to facilitate further harmonisation across Member States of data mining tools.

**Recommendation 3:** The Commission should engage in communication activities with Member States on how to use data tools such as Arachne and EDES. Such communication would also allow the Commission to understand Member States’ reservations behind not using these tools and amend them where appropriate.

**Recommendation 4:** The EU data collection and risk analysis tools should be better integrated. Furthermore, the same tools should be available for all EU funding programmes (e.g. all shared management funding such as cohesion, employment, research and development, agricultural and regional funds).

**Networking and the sharing of information**

There are a number of networks at the EU level that allow Member States and OLAF to exchange experience and good practices on fraud prevention and tackling organised crime. These include EMPACT, COCOLAF, and the Working Group on Combating Fraud. Nevertheless, although useful, some
Member States have indicated that these networks are sometimes not relevant to their specific situations due to differing levels of organised crime and fraud across the EU. Therefore, in addition to these EU-wide networks (and not replacing them), regional networks could be launched to bring together Member States which are likely to be involved in the same cross-border cases of fraud and organised crime and which have similar experiences. On the other hand, some Member States may find it burdensome to engage in both EU level networks and regional networks. Member States are therefore encouraged to establish these networks on a case-by-case basis if it is of interest to them.

Recommendation 5: Member States are encouraged to establish regional cooperation networks for groups of Member States to share information on cases and strategies to combat fraud against the EU finances if it is of interest to them. Such regional cooperation networks would allow Member States to obtain best-practice and information that is more relevant to the cases being dealt with by national authorities. Regional (in addition to EU-wide) networking would make it easier to focus on the priorities of specific countries as well as fostering cooperation in tackling fraud where there is a transnational dimension.

Extending jurisdiction and increasing the confiscation rate

Although prevention is the most effective way of combating fraud against the EU’s finances, increasing the confiscation rate of criminal profits has a strong deterrent effect but there are difficulties in doing this when the proceeds are offshore. Feedback from the research indicates that to increase the confiscation rate of criminal profits, and combat cases of money laundering of defrauded EU funds through offshore accounts, the EU should adopt an approach similar to the extraterritorial approach adopted by the US authorities. Under this approach, the US authorities have jurisdiction over dollar-denominated transactions regardless of the country in which the money laundering is occurring. It was indicated that this is partly in line with Article 11 of the PIF Directive which says that “Each Member State shall take the necessary measures to establish its jurisdiction over the criminal offences referred to in Articles 3, 4 and 5 where: (a) the criminal offence is committed in whole or in part within its territory; or (b) the offender is one of its nationals.” Furthermore, Article 11(2) and (3) provide for optional avenues for Member States to “extend its jurisdiction” on crimes against the EU’s financial interests. Since the money laundering of criminal funds in offshore accounts remains an issue, efforts need to be made to ensure that EU jurisdiction is established over third countries holding these accounts.

Recommendation 6: In line with Article 11 of the PIF Directive, the Commission and Member States should ensure that their jurisdiction is established over criminal offences against the EU’s financial interests occurring in third countries. Member States should introduce laws that bring their rules in line with Article 11 to ensure extended jurisdiction. The Commission on the other hand should make efforts to ensure Member States have complied with these obligations and encourage them to prosecute and investigate cases involving third countries. Ensuring such jurisdiction is established would make it easier for the EPPO (and Member States not participating in the EPPO) to prosecute cases of fraud in which money is laundered outside of the EU. Considering that criminal profits are quickly moved out of the EU this would also help to increase the confiscation rate which is important for deterring organised crime from engaging in this activity.
Closing loopholes in the VAT system

The current VAT system has gaps that make it particularly vulnerable to fraud, particularly Missing Trader Intra-Community (MTIC) Fraud. Due to the complex nature of MTIC fraud, it is estimated that almost all of this type of fraud is committed by organised crime groups. As indicated earlier, one estimate is that 80% of VAT fraud is committed by 2% of organised crime groups. Therefore, in order to combat fraud and organised crime’s impact on EU financial interests, the intra-community VAT system needs to be updated to close the loopholes that organised crime groups make use of to defraud the EU.

**Recommendation 7:** The intra-community VAT system should be updated to close loopholes that can be exploited by organised crime through MTIC schemes. Legislative solutions which allow for the payment of VAT across EU borders without the potential for ‘Missing Traders’ to disappear with the VAT owed to Member States would remove a key way in which EU and national financial interests are defrauded by organised crime.

The shortcomings of anti-fraud and control measures used by national authorities responsible for the management of EU funds increases the risk of fraud. Despite this being the case, the implementation of effective anti-fraud measures was not considered among the “enabling conditions” criteria stipulated by the Commission Delegate Regulation for 2014-2020 nor is it mentioned in that for 2021-27\(^{123}\). Strengthening the requirement for effective and proportionate anti-fraud measures as a condition for Managing Authorities to be able to access EU funding would constitute a major step in the effort against fraud and strengthen the anti-fraud framework.

**Recommendation 8:** The EU should set common quality standards for national anti-fraud systems and reporting procedures and require a declaration of compliance. This would help ensure that managing authorities develop robust control systems to manage EU funds. Member States all have different national strategies to tackle fraud. While each Member State faces a different regional context when it comes to fraud and organised crime, minimum standards established across the EU would help ensure fraud an emphasis on working towards best practices.

### 5.3 Conclusions and Recommendations – Member States

EU Member States are responsible under shared management for controlling most of the EU expenditure and revenue-raising. However, the capacity of national authorities to address the challenge of organised crime in relation to the EU finances varies considerably across the EU Member States and while some have well-developed strategies, resources and mandates, others do not. This also creates challenges and obstacles for efficient cooperation. Differences between Member States in terms of reporting on fraud and irregularities arise because of differences in national systems to counter fraud as well as non-harmonised reporting systems. Similarly, the EU level tools to detect and prevent fraud are not used by all Member States or are not used extensively by some others. An additional complication is that there is no distinction in some Member States between national financial crimes and EU financial crimes. This study suggests that a key priority is to develop a common approach to estimating the level of fraud affecting the EU finances and in relation to the measures taken by Member States to tackle the problem.

---

Improving early detection

The early detection of suspected fraud cases – especially prior to disbursement of EU funds - is still a challenge for many Managing Authorities. But the capacity to detect likely cases early is a key to tackling fraud. MAs are expected to assess fraud risks in relation to public procurement they manage directly (e.g. in the context of technical assistance) or indirectly. In 2014, the Commission encouraged MAs to adopt a proactive and targeted approach to managing the risk of fraud in programmes and provided guidelines and a self-assessment instrument for this purpose. Effective fraud risk assessment is the basis of the prevention and early detection of fraud. However, the effectiveness of fraud risk assessment approaches and control systems vary across the EU. Some national authorities have introduced fraud indicator checklists (e.g. related to conflict of interests of the authorities' staff, controls in the form of 'red flag' risks, and dedicated risk assessment task forces).

Recommendation 9: Member States need to develop effective fraud risk assessment and management systems to help ensure the early detection and reporting of fraud risks. To help achieve this, Member States could benefit from the use of Arachne in public procurement procedures, the implementation of the Commission guidelines and recommendations relating to programmes and the systematic use of the PIF Reports’ findings in relation to national fraud risk assessments. More needs to be done to ensure that fraud risk assessment approaches are regularly reviewed to address new emerging fraud risks.

Capacity building

Capacity building is needed to help national authorities in some Member States to develop more effective ways of combatting organised crime fraud against the EU’s finances. Guidelines and training should be provided to Managing Authorities and other competent bodies on how to assess, detect and report fraudulent cases in line with EU requirements. This would help ensure a more uniform system for data collection, standardise the reporting process and improve the quality and comparability of data provided both to the EU level. Some national authorities have indicated that training courses have in some cases also involved judicial and administrative authorities that work alongside MAs in dealing with cases of suspected fraud. Training sessions could also involve OLAF, the AFCOS and international organisations such as the OECD, partly to ensure best practice is shared more widely. The sessions could focus on topics such as: raising awareness of the fraud risks; ensuring an understanding of the legal basis for combating fraud against the EU finances; investigating the modus operandi of criminal groups; and sharing good practices on how to detect fraud. Providing clear and detailed guidance to national authorities is also key to enhance the capacity to assess, prevent, detect and combat fraud and corruption in EU investment and structural funds.

Furthermore, it has been highlighted that the contrast between the lack of understanding of organised crime’s involvement in fraud of EU expenditures on the one hand, and the understanding that most of EU revenues fraud is committed by organised crime on the other, could be explained by the different resources available to the authorities handling these cases of fraud. When it comes to identifying revenue fraud, law enforcement and border forces are involved whilst for expenditures, it is often only the managing authorities of EU funds. Member States are therefore encouraged to develop and strengthen the capacity of authorities managing EU expenditures to detect, investigate and report fraud. This could involve training as well as recruiting additional staff competent in this field.

124 Fraud Risk Assessment and Effective and Proportionate Anti-Fraud Measures - Regional Policy - European Commission (europa.eu)
**Recommendation 10:** Supported by the EU, Member States should be encouraged to provide training to staff of the relevant authorities to equip them with the knowledge to identify potential fraud, make use of the relevant tools effectively and report suspicious cases in line with EU standards. This should also be done with a view to enhancing the capacity of authorities managing EU funds to detect, investigate and report fraud. This is particularly with the case of data tools such as EDES and Arachne where training schemes for the national authorities would help them understand how to use tools identified by the EU to full effect.

**Role of the AFCOS**

Current EU legislation supporting the AFCOSs defines their mandate and role in very general terms and this has led to a situation where their role and capabilities vary considerably from one country to another. As a minimum, AFCOs should facilitate effective cooperation and the exchange of information with OLAF. Additional guidance by the European Commission\(^{125}\) specified they should be responsible for coordinating all administrative and legislative measures related to the protection of the EU’s financial interests within the national territory. However, it is up to the individual Member State to determine the specific characteristics and competences of its AFCOS and this has resulted in significant differences in the structure, role and responsibilities across Member States. In addition to being a contact point for OLAF, Member States would benefit from strengthening the AFCOSs’ coordination role at a national level in relation to fraud cases under investigation involving EU funding. In many cases, AFCOSs do not have a comprehensive overview of all investigations that may be taking place. Rectifying this would not only strengthen the efforts to combat fraud at a national level but also improve the quality of information available to OLAF at the EU level.

**Recommendation 11:** The European Commission should define minimum standards for AFCOSs and Member States should adopt these standards to help harmonise their effectiveness across the EU. These standards should include the responsibility to have a comprehensive overview of cases of fraud affecting EU finances under investigation by all competent authorities at the national level and to help coordinate such information sharing. Additionally, the AFCOSs’ role could be extended to include being a liaison point for the Advisory Committee for the Coordination of Fraud Prevention (COCOLAF) of the Commission and the Working Group on Combating Fraud of the European Council.

**Prioritising measures to combat fraud against the EU’s finances**

Feedback from the research suggests that in some countries, efforts to combat fraud involving EU funds tend not to be prioritized to the same extent as fraud involving purely national expenditure. This is highlighted by the fact that more than half of OLAF investigations are not followed up by Member States and even less reach the prosecution stage. The creation of the EPPO is expected to increase the number of fraud and organised crime cases that are investigated and prosecuted. Likewise, under the latest Commission Anti-Fraud Strategy, OLAF is to be provided with a more centralised oversight role which inter alia will require Member States to give reasons for not following up OLAF recommendations. Nevertheless, it is clear that national authorities should do more to follow up cases indicated by OLAF of possible fraud against the EU’s finances. In this respect, Member State

\(^{125}\) Guidance note on main tasks and responsibilities of an Anti-Fraud Coordination Service (AFCOS), 13 November 2013, Ares (2013) 3403880
authorities can refer cases to Eurojust for the facilitation of the cooperation and coordination at the judicial level.

**Recommendation 12: Member States should take up more of the cases highlighted by OLAF of possible fraud against the EU’s finances.** The creation of the EPPO should help increase the success rate in prosecutions and the recovery of defrauded funds. Nevertheless, Member States still have responsibility in areas where the EPPO does not have the competency to intervene, for example when a case of VAT fraud occurs in only one Member State. Furthermore, considering the large scale of fraud, Member States should continue to investigate and prosecute cases alongside the EPPO to tackle the issue.

**Engaging civil society and the private sector in combating fraud**

Broadening the approach by also involving civil society and the private sector would strengthen the fight against fraud. At present, irregularities are most often detected through checks by the programme management authorities such as the MAs, certifying authorities, auditors and prosecutors. The media also has an important role to play. However, more could be done to involve civil society and the private sector which would strengthen the fight against fraud. National authorities could, for example, set up online communication channels through which citizens could anonymously report suspected cases of fraud related to EU funded projects. Examples of this exist in Latvia\(^\text{126}\), Finland and in Spain, although in the latter case this is not anonymous, and individuals are ensured confidentiality but need to identify themselves. The authorities would of course need to guarantee anonymity and protection for those coming forward with suspected cases of fraud, for example through the full implementation and possibly the expansion of the Whistle-blower Directive. The Integrity Pacts piloted by the European Commission alongside Transparency International in Latvia, Romania and Hungary are another example of what can be done to involve civil society. The pacts involve agreements in which the authority responsible for awarding a public contract and economic operators agree to abstain from corrupt practices, and monitoring tools were used to monitor compliance and enhance transparency.

**Recommendation 13: Member States should seek to involve civil society as well as the private sector in the effort to combat fraud. This would include developing confidential channels to report suspected fraud and to guarantee protection to those doing so.** Furthermore, involving civil society and the private sector in the fight against fraud and organised crime would help ensure that expertise in this third sector that is not found in the EU institutions or Member States currently is fully mobilised in the EU’s fight against fraud.

**Improving estimates of organised crime fraud and the effectiveness of countermeasures**

National level authorities only have a very partial picture of the extent to which organised crime is involved in defrauding EU finances. Several national authorities indicated that they do not gather data on the extent to which organised crime is involved in fraud cases on the expenditure side of EU finances. On the other hand, the authorities handling EU revenues, for example intra-community VAT, seem to have a clearer picture when it comes to organised crime’s involvement in defrauding EU resources. As noted earlier, almost all of MTIC fraud is thought to be committed by organised crime groups. Considering the lack of knowledge, and the risk that organised crime will attempt to take

---

\(^\text{126}\) [https://atkrapies.lv/zino-par-parkapumiem/](https://atkrapies.lv/zino-par-parkapumiem/)
advantage of the Next Generation EU recovery funds, it is important that more research is undertaken on the extent to which organised crime has infiltrated in EU expenditure programmes.

| Recommendation 14: Member States supported by OLAF and the EPPO where appropriate, should undertake research to improve the estimates of the financial impact of organised crime fraud involving the EU’s finances, particularly when it comes to EU expenditure. This could be done in partnership with international organisations so as to ensure a harmonised approach by Member States and a joint effort in their fight against organised crime. |

The study research suggests that the AFCOS and relevant national authorities involved in investigations of fraud against the EU finances often do not monitor or evaluate the effectiveness of anti-fraud measures. This makes an evidence and results-based approach to adjusting national anti-fraud strategies and policies difficult. Closer monitoring of ongoing and new anti-fraud measures in relation to prevention and detection, and the effectiveness actions taken by AFCOSs, MAs and other entities would help Member State advance their efforts against fraud to the EU’s financial interest and do so in a comprehensive, evidence-based manner. These components of anti-fraud systems should also be reviewed on a regular basis to address emerging risks and target sophisticated criminal organisations and networks.

| Recommendation 15: Member States should with EU guidance as appropriate, regularly evaluate their anti-fraud frameworks to establish their effectiveness, identify best practices and review their anti-fraud strategies to address any emerging risks. Independent reviews of the anti-fraud frameworks would help ensure Member States are consistent in adopting high standards in the fight against fraud and also help to identify best-practices in these Member States and/or help them adopt such policies from elsewhere. |
ANNEX A: LIST OF SECONDARY SOURCES

- EU Strategy to tackle Organised Crime 2021-2025
- 2020 Rule of Law Report
- Serious and Organised Crime Threat Assessment (SOCTA)
- OECD - Fraud and corruption in European Structural and Investment Funds. A spotlight on common schemes and preventive actions (2019)
- OECD – Effective Inter-Agency Co-operation in Fighting Tax Crimes and Other Financial Crimes
- European Commission – Arachne Risk Calculations
- European Court of Auditors – Tackling fraud in EU cohesion spending: managing authorities need to strengthen detection response and coordination
- European Court of Auditors – Special report Fighting fraud in EU spending: action needed
- European Court of Auditors – Customs controls: insufficient harmonisation hampers EU financial interests
- European Court of Auditors – E-commerce: many of the challenges of collective VAT and customs duties remain to be resolved
- European Court of Auditors – Customs controls: insufficient harmonisation hampers EU financial interests
- SWD(2021) 74 final: EMPACT, the flagship EU instrument for cooperation to fight organised and serious international crime
- OLAF - Opinion No 1/2021 OLAF’s recommendations not followed by the relevant authorities
- Europol: Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU (April 2020).
- COM(2020) 605 final EU Security Union Strategy
- Fazekas, Mihály, and King, Peter Lawrence, (2019), Perils of development funding? The tale of EU Funds and grand corruption in Central and Eastern Europe. Regulation & Governance, 13(3).
- OLAF. (n.d.). The annual OLAF reports of the European Anti-Fraud Office.
Impact of Organised Crime on the EU’s Financial Interests

- PWC. (2011). How does organised crime misuse EU funds?
- Rand Europe (2016), The Cost of Non-Europe in the area of Organised Crime and Corruption, European Parliamentary Research Service. European Added Value Unit, PE 579.319

Section 4 References

- Caneppele, Stefano & Martocchia, Sara. (2014). Italian Mafias, Public Procurement and Public Works in Southern Italy. 10.1007/978-3-319-01839-3_33.
ANNEX B: MODELING METHODOLOGY

Predictive model of OC infiltration in public procurement

The model was developed using two Italian administrative data sources: 1) database of dissolutions of local governments in Italy due to OC infiltration; 2) database of public procurement tenders with a reserve price higher than 150000 euros for the period 2008-2014, managed by the ANAC, the Italian anticorruption agency.

The first source included dates of dissolutions of local governments in Italy. The dataset with public procurement tenders provides information on the auction ID, number of bidders, bidders’ names, bids, contract awarding procedure, the reserve price of the contract, the categories of work involved in the contract, and the final price paid by the contracting authority and the timing for the completion of the project.

The two outlined datasets were matched to construct a data set for analysis that included tenders of more than 1,500 Italian municipalities over the period 2008–2014, as well as binary indicator of the OC infiltration at the contract level. The binary indicator of the OC infiltration classified tenders to two groups based on the dates of dissolutions: 1) the tenders that were awarded in the period prior to the dissolution were marked as most likely influenced by OC; 2) the tenders that were awarded in the period after the dissolution were marked most likely not influenced by OC.

The resulting dataset was updated with the additional variables:

- NUTS3 regions-level features: population, area size, coast, mountain and capital statuses.
- Date attributes: date of the week, week of the month, month, quarter.

Table B1: Overview of variables used in the analysis

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Variable Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Procurement-related indicators</strong></td>
<td></td>
</tr>
<tr>
<td>Log contract value</td>
<td>Logarithm of the awarded value.</td>
</tr>
<tr>
<td>Number of bids</td>
<td>Number of bids submitted, trimmed at 20.</td>
</tr>
<tr>
<td>CPV division</td>
<td>First two digits of the main CPV code of the tender (XX000000-Y).</td>
</tr>
<tr>
<td>Selection criterion</td>
<td>Whether the main criterion for winner selection is the lowest price or MEAT.</td>
</tr>
<tr>
<td>Contract delivery is local</td>
<td>Whether the location of contract implementation is the same as the buyer’s location (y = 1), or not (y = 0).</td>
</tr>
<tr>
<td>Consortium</td>
<td>Whether tender winner is a member of consortium (y = 1) or not (y = 0)</td>
</tr>
<tr>
<td>Supple type</td>
<td>Whether procurement type is services, works or supplies.</td>
</tr>
<tr>
<td>Framework agreement</td>
<td>Whether a procurement procedure is a framework agreement (y = 1) or not (y = 0).</td>
</tr>
<tr>
<td>Administrative error</td>
<td>Share of missing key values (information about winner, buyer, contract value, number of bids) in the tender.</td>
</tr>
<tr>
<td>Share of supplier in buyer’s annual spending</td>
<td>Calculated as a share of total contract value of the winner in the year divided by total contract value awarded by the procuring entity in the year.</td>
</tr>
</tbody>
</table>
A set of alternative predictive models - logistic regression, Random Forest, and Gradient Boosting Machines - were estimated and the best method selected based on prediction accuracy. Models were compared based on the percent correctly classified contracts on the test dataset with 70% of the sample used for training the models and 30% used for testing accuracy.

### Table B2: Accuracy of the models of predicted probabilities of OC infiltration

<table>
<thead>
<tr>
<th></th>
<th>Logistic regression</th>
<th>Random Forest</th>
<th>Boosting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prediction Accuracy on Test Set</td>
<td>71%</td>
<td>89%</td>
<td>88%</td>
</tr>
</tbody>
</table>

Based on the percent correctly classified contracts, the Random Forest classifier model was selected as the best performing model. This model was trained using R package “randomForest”\(^{127}\). The model’s hyperparameters are as follows: the number of decision trees - 1000, the number of variables randomly sampled as candidates at each split - 14.

The selected model was used to make the EU-wide prediction of OC infiltration risk score using micro-level dataset of public procurement in the EU.

---

\(^{127}\) [https://cran.r-project.org/web/packages/randomForest/randomForest.pdf](https://cran.r-project.org/web/packages/randomForest/randomForest.pdf)
**Price modelling**

Figure B1: Predicted probabilities of SOC infiltration at the contract level, sample is restricted to the contracts awarded by municipalities

![Histogram of predicted probabilities](image1)

Figure B2: Predicted probabilities of SOC infiltration at the contract level, sample is restricted to the EU-funded contracts awarded by municipalities

![Histogram of predicted probabilities](image2)

Table B3: Summary statistics of SOC infiltration score, sample is restricted to the EU-funded contracts awarded by municipalities

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>Median</td>
<td>Min</td>
<td>Max</td>
<td>St. Dev.</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>0.274</td>
<td>0.268</td>
<td>0.019</td>
<td>0.663</td>
<td>0.09</td>
<td>85781</td>
<td></td>
</tr>
</tbody>
</table>
ANNEX C: COUNTRY FACTSHEETS

Please see stand-alone document:
This analytical study examines the impact of organised crime on EU’s finances. Taking together the expenditure and revenue sides, the research suggests that between 1% and 2% of the EU budget is defrauded each year. The study also assesses measures at the EU and Member States’ levels to combat the problem and recommends actions to help reinforce these measures. The study was requested by the European Parliament’s Committee on Budgetary Control.