Council of the European Union

Brussels, 29 January 2018
(OR. en)

5724/18

Interinstitutional File:
2017/0226 (COD)

DROIPEN 12
CYBER 17
JAI 53
TELECOM 23
MI 54
IA 32
CES 1
CODEC 109

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	23 January 2018
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
Subject:	OPINION of the European Economic and Social Committee - Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA [12181/17 DROIPEN 120 CYBER 126 JAI 784 TELECOM 206 MI 626 IA 138 CODEC 1400 - COM(2017) 489 final]

Delegations will find attached the above-mentioned opinion.

European Economic and Social Committee

INT/831
Combating fraud and counterfeiting of non-cash means of payment

OPINION

European Economic and Social Committee

Proposal for a directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA
[COM(2017) 489 final – 2017/0226 (COD)]

Rapporteur: **Victor ALISTAR**

Consultation	European Parliament, 02/10/2017 Council, 25/10/2017
Legal basis	Article 83(1) of the Treaty on the Functioning of the European Union
Section responsible	Single Market, Production and Consumption
Adopted in section	18/12/2017
Adopted at plenary	18/01/2018
Plenary session No	531
Outcome of vote (for/against/abstentions)	129/0/1

1. **Conclusions and recommendations**

1.1 The EESC welcomes the Commission's initiative to prioritise the fight against cybercrime – a form of crime targeting electronic payment instruments – even though this should have been made a priority a long time ago. The benefits of digitisation must be flanked by mechanisms able to meet the accompanying challenges, so that the European economy and Europeans can enjoy the information society to the full. The EESC endorses the Commission proposal, as it aims to protect Europeans and businesses from cybercrime networks, and includes measures to boost confidence in the use of electronic payment instruments.

1.2 On analysing the proposal for a directive, the EESC finds that a number of shortcomings need to be addressed and corrected:

1.2.1 In Article 11 on jurisdiction of investigation, it must be clarified whether the fundamental principle is the location of the person or of the computer or information system used in order to avoid a conflict of jurisdiction. The EESC asks that a subpoint be added to Article 11 on settling conflicts of jurisdiction using one of the two methods suggested.

1.2.2 The proposal for a directive does not fully consider a situation involving other non-EU jurisdictions as well, or mechanisms for referring to other legal instruments for international judicial cooperation, and so a predictable and clear procedural framework must be established.

1.2.3 Article 16 on prevention should include specific measures, stipulated in the Member States' transposition legislation, regarding the requirement to provide information. This requirement would have to be met either by providers of electronic payment products or by national regulatory authorities, or by those responsible for financial education.

1.2.4 In conjunction with Articles 12 and 13, provision must be made for the exchange of best practice with regard to detecting, investigating and dealing with cases of cybercrime involving electronic means of payment fraud.

1.3 Although the area of regulation here is part of investigative and judicial cooperation in the area of cyberfraud, it is important to establish deterrents and mechanisms to inform the public about the modus operandi of offenders as well, through awareness-raising campaigns conducted by law enforcement authorities in the Member States.

1.4 In order to ensure efficient protection of individuals and to meet the objectives behind this initiative (namely, boosting confidence in electronic and digital payment instruments and increasing compliance and prevention), Article 15 must require national legislation to institute financial insurance against fraud, so that victims are compensated fully should the holders of electronic payment instruments be harmed by cyberfraud. This compensation would be paid out to the payment product provider, as the civil plaintiff concerned, upon completion of the investigation.

1.5 In order to make the policy on combating the counterfeiting of electronic payment instruments both efficient and effective, a requirement to report incidents involving counterfeited electronic

payment instruments must be built into the directive, as it is in the case of policies on combating money laundering or the regulation on personal data protection.

1.6 The EESC points to the need to increase our capacity to understand and prevent digital and electronic payment instrument fraud by setting up a system for gathering statistics that would bolster strategies aimed at preventing and remedying the effects of such fraud. Furthermore, there should be an ongoing impact assessment of the measures taken by the Member States to transpose the directive, with quantitative reporting on an annual basis and a qualitative impact assessment every two or three years, so as to ascertain how effective the policy is and whether it needs to be adjusted.

1.7 With a view to making the fight against cyberfraud and counterfeiting of payment instruments more effective in the medium term, Article 16 should be reinforced by clearly stipulating that Member States are required to build up expertise in this area, developing investigative experience and the exchange of experience, in order to enhance the broad spectrum skills of graduates (through optional studies) and the skills of experts and investigators (through specialised ongoing training).

1.8 Moreover the Committee is of the opinion that cooperation on the ground is absolutely essential and should be encouraged. This concerns both national and cross-border cooperation for combating or preventing this type of crime. All stakeholders, in both the public and private sectors, should be involved here.

1.9 There may be some confusion regarding the subject of this directive, and so we would propose altering its title and replacing the phrase *non-cash means of payment* with *electronic and digital means of payment*.

2. Commission proposal

2.1 The purpose of the directive is to ensure uniformity between the relevant instruments and increase the ability of Member States to investigate fraud committed using digital or electronic means of payment. The proposal focuses on cross-border cooperation between investigating authorities and a set of relevant measures, as well as common minimum standards on prevention, assistance to victims and the responsibility of the issuers of these instruments. In this respect, the approach taken is to define the scope of the instrument, which aims to provide a technology-neutral perspective.

2.2 Given the technological developments and diversification in modus operandi in the field of cyberfraud, including in strategies used by groups of offenders, the Commission acknowledges in the EU Agenda on Security[1] that the Framework Decision insufficiently addresses new challenges and technological developments such as virtual currencies and mobile payments.

2.3 Cards are the most important non-cash payment instrument in the EU in terms of number of transactions, and fraud involving cards issued in the euro area reached EUR 1.44 billion in 2013

[1] Commission communication on *A Digital Single Market Strategy for Europe*, COM(2015) 192 final.

according to a European Central Bank study, and continues to grow[2]. Although fraud data exist only for card payments, cards are the most important non-cash payment instrument in the EU in terms of number of transactions[3].

2.4 The Commission analysis shows that one of the areas most vulnerable to fraud is electronic payment of travel expenses, train and plane tickets, accommodation and related transactions, along with various other payments.

2.5 The Commission proposal aims to ensure that a robust and technology-neutral legal framework is in place, to eliminate operational obstacles and to enhance prevention of fraud involving electronic means of payment.

2.6 With a view to providing efficient means to combat electronic payment instrument fraud and cybercrime, the proposal for a directive establishes common standards for national legislation on: offences covered by criminal legislation on cyberfraud involving means of payment; participation in offences and criminal policy establishing penalties; liability of legal persons and the establishment of uniform dissuasive penalties. The EESC would note one particular novelty here: this is the first move to regulate virtual currencies in EU law. The definition of offences covers behaviours which do not immediately constitute the actual fraud, but which are committed in preparation for fraud (stealing and counterfeiting, but also sale and mere possession of stolen payment instruments).

2.7 In order to enhance European cooperation on combating cybercrime and electronic payment instrument fraud, the directive aims to establish specific, relevant provisions for institutional mechanisms and investigative jurisdictions in the Member States, as well as for the European mechanism for the exchange of information between national authorities.

2.8 One key element is the requirement to establish efficient means of safeguarding the interests of victims and provide access to an effective remedy.

2.9 The Commission proposal falls fully within the legislative scope of the European Union, in accordance with Article 83 of the Treaty on the Functioning of the European Union, and calls for minimum harmonisation between the Member States with a 24-month transposition period.

3. General comments

3.1 The legislative option chosen is much more suitable, since a directive can establish standards which will be binding upon all national jurisdictions (with the exception of Denmark, if it does not join on a voluntary basis). This will do much more than standardise practices, as laid down in Framework Decision 2001/413/JHA, without affecting the content of the framework decision.

---

2 European Central Bank, *Fourth report on card fraud*, July 2015 (most recent data available).

3 See footnote 2.

3.2 The EESC notes that the proposal for a directive is in synergy with other regulatory instruments to which the Member States are party and complements other EU policies, such as pan-European mechanisms on cooperation in criminal matters and combating cyberfraud or money laundering. In this context, it must be pointed out that this needs to be linked both to methods of protecting personal data held by financial institutions and to cybersecurity measures.

3.3 Basically, there are a number of legal instruments at EU level laying down standards applicable to the financial market and financial services and stipulating the requirement to exercise due diligence when providing, managing and securing payment instruments, and the proposal for a directive contributes to the construction of a stronger legal infrastructure for reporting, investigating and sanctioning cyberfraud involving means of payment.

3.4 The EESC points to the need to increase our capacity to understand and prevent digital and electronic payment instrument fraud by setting up a system for gathering statistics that would bolster strategies aimed at preventing and remedying the effects of such fraud. Furthermore, there should be an ongoing impact assessment of the measures taken by the Member States to transpose the directive, with quantitative reporting on an annual basis and a qualitative impact assessment every two or three years, so as to ascertain how effective the policy is and whether it needs to be adjusted.

3.5 Similarly, given that liability of legal persons and penalties will be established by a more robust mechanism for guaranteeing legal means, it must be reiterated[4] that operators providing electronic payment products or using online payment platforms must be given support to comply with sectoral regulations[5].

3.6 As regards the mechanism for information exchange on investigations into cybercrime involving payment instrument fraud, as laid down in Articles 13 and 14 of the proposal for a directive, provision must be made to empower the Commission to use delegated acts to regulate the information exchange mechanism and standardised reporting data on ongoing cases.

3.7 As regards prevention, although the Commission communication refers to a similar approach to that taken by Directive 2011/93/EU, the EESC considers that there is a need for greater clarity regarding obligations with regard to prevention, and for the introduction of mandatory awareness-raising activities with regard to causes, risks and individual means of prevention in order to avoid financial payment instrument fraud arising from traps laid by cybercrime networks.

3.8 Expertise in this area must be built up, developing investigative experience and the exchange of experience, in order to enhance both the broad spectrum skills of non-specialised graduates through optional studies and a competency framework for experts and investigators through specialised ongoing training.

---

4 See previous EESC opinions.

5 OJ L 267, 10.10.2009, p. 7.

3.9 It is important that there be effective cooperation on the ground in order to counter this type of crime. Cooperation must be organised in different domains and all stakeholders involved as much as possible. This should make it possible to combat but also prevent this serious form of crime. This applies at both national and cross-border level.

3.10 The proposal for a directive does not fully consider a situation involving other non-EU jurisdictions as well, or mechanisms for referring to other legal instruments for international judicial cooperation, and so a predictable and clear procedural framework must be established.

3.11 Although the area of regulation here is part of investigative and judicial cooperation in the area of cyberfraud, it is important to establish deterrents and mechanisms to inform the public about the modus operandi of offenders as well, through awareness-raising campaigns conducted by law enforcement authorities in the Member States. In this respect, the final provisions of the proposal should specify the instruments for international judicial cooperation in criminal matters that will be referred to in extraterritorial situations and the manner in which investigations will be conducted using these instruments. In terms of procedure, this is a useful regulatory tool that can clarify the situation.

4. Specific proposals

4.1 In Article 11 on jurisdiction of investigation, it must be clarified whether the fundamental principle is the location of the person or of the computer or information system used in order to avoid a conflict of jurisdiction between the situation described in Article 11(2)(a), regarding physical presence, and the situation in Article 11(2)(b), if the person has committed the offence in the territory of a Member State but used a remote shell programme. This could mean that both EU Member States have jurisdiction. A subpoint should be added to Article 11 on settling conflicts of jurisdiction, either by identifying the competent body (such as EUROJUST) or by referring the matter to a similar settlement mechanism (such as Framework Decision 2009/948/JHA[6]).

4.2 Article 16 on prevention should include specific measures, stipulated in the Member States' transposition legislation, regarding the requirement to provide information. This requirement would have to be met either by providers of electronic payment products or by national regulatory authorities, or by those responsible for financial education.

4.3 With regard to the requirement to establish a mechanism for the exchange of information regarding fraud investigations, laid down in Article 13 of the proposal of a directive, a single contact point must be identified, similar to the one for combating money laundering or upholding food safety, so as to ensure a standardised approach across the EU. This single contact point could be the ministry of justice or another body common to most EU jurisdictions. The EESC considers that while the phrase "appropriate […] channels" goes some way towards meeting the need for efficiency, it fails to meet the need for a standardised approach.

6 OJ L 328, 15.12.2009, p. 42.

4.4 In conjunction with Articles 12 and 13, provision must be made for the exchange of best practice with regard to detecting, investigating and dealing with cases of cybercrime involving electronic means of payment fraud.

4.5 In order to ensure efficient protection of individuals and to meet the objectives behind this initiative (namely, boosting confidence in electronic payment instruments and increasing compliance and prevention), Article 15 must require national legislation to institute financial insurance against fraud, so that victims are compensated fully should the holders of electronic payment instruments be harmed by cyberfraud. This compensation would be paid out to the payment product provider, as the civil plaintiff concerned, upon completion of the investigation. Such safeguards must cover damage caused to traders represented by SMEs in the event of failure to settle amounts up to a reasonable ceiling, determined at Member State level.

4.6 In order to make the policy on combating the counterfeiting of electronic payment instruments both efficient and effective, a requirement to report incidents involving counterfeited electronic payment instruments must be built into the directive, as it is in the case of policies on combating money laundering or the regulation on personal data protection.

Brussels, 18 January 2018

Georges Dassis
The president of the European Economic and Social Committee