Briefing

Initial Appraisal of a European Commission Impact Assessment

European Parliament

December 2017

Combating fraud and counterfeiting of non-cash means of payment

Impact assessment (SWD(2017) 298, SWD(2017) 299 (summary)) of a Commission proposal for a directive of the European Parliament and the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (COM(2017) 489)

Background

This note seeks to provide an initial analysis of the strengths and weaknesses of the European Commission's impact assessment (IA) accompanying the above proposal, submitted on 13 September 2017 and referred to Parliament's Committee on Civil Liberties, Justice and Home Affairs.

The current legal framework that establishes common minimum rules on the criminalisation of non-cash payment fraud and counterfeiting is Council Framework Decision 2001/413/JHA. The framework decision was part of the 2001 EU Action Plan on preventing fraud and counterfeiting of non-cash means of payment. However, the policy and legislative contexts have significantly changed since 2001 and various legislative acts have been adopted at EU level to secure payments and prevent fraud and counterfeiting. Among them are:

- the Payment Services Directive 2015/2366/EU;
- the Attacks Against Information Systems Directive 2013/40/EU;
- the Fourth Anti-Money-Laundering Directive 2015/849/EU and the proposal amending it;
- Directive 2014/62/EU on the protection of the euro and other currencies against counterfeiting by criminal law;[1]
- Directive 2012/29/EU on the rights, support and protection of victims of crime.

In addition to this, the volume of online transactions and the use of non-cash payment methods have been increasing in Europe in recent years. Against this background, in its resolution of 2013[2] the European Parliament called for common definitions and harmonisation of regulations concerning electronic and mobile money products as regards their potential use for money laundering and terrorist financing purposes. In its more recent resolution of 2017[3] the European Parliament stresses the importance of harmonisation at the EU level of the definition of offences linked to attacks against information systems and the need for the Member States to set up systems for the recording, production and provision of statistical data on related offences, in order to fight against crime more effectively. In the European Agenda on Security of April 2015, the European Commission announced its intention to adopt the legislation on combating fraud and counterfeiting of non-cash means of

[1] A. Maniaki-Griva, Protection of the euro and other currencies against counterfeiting by criminal law, initial appraisal of a Commission impact assessment, EPRS, European Parliament, May 2013.
[2] European Parliament resolution of 23 October 2013 on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken, P7_TA(2013)0444.
[3] European Parliament resolution of 3 October 2017 on the fight against cybercrime, P8_TA-PROV(2017)0366.

EPRS | European Parliamentary Research Service
Author: Vera Vikolainen
Ex-Ante Impact Assessment Unit
PE 611.031

payment by December 2016. The Commission included the proposal in its 2016 work programme under the new initiatives, but later re-scheduled it for autumn 2017 when it was finally adopted (13 September 2017).

Problem definition

The problem definition provided in the IA builds on the evaluation[4] of Framework Decision 2001/413/JHA presented in Annex 5 (IA, pp. 194-234). The main problem identified is **non-cash payment fraud**, which is caused by three main problem drivers, divided into various sub-drivers (IA, pp. 19-30). These are summarised below:

1. Deficiencies of the current legal framework

The framework decision covers physical payment instruments (i.e. cards, cheques, travellers' cheques, bills of exchange) and does not explicitly include non-physical payment instruments such as virtual currencies, e-money and mobile money; neither does it include any definition of computer data or computer programme/system. It covers the fraudulent use of payer information, but does not cover preparatory acts that precede fraud, such as the collection (e.g. phishing, skimming), trade, making available and possession of payer information. The framework decision requires Member States to set up criminal penalties that are effective, proportionate and dissuasive, without specifying minimum levels. Finally, the framework decision provides limited tools to address the challenges of allocating jurisdiction due to the cross-border nature of the crime.

2. Operational obstacles

It can take too long to receive and to provide the information requested from or to another Member State. The framework decision requires Member States to designate operational contact points for the exchange of information, but does not specify who those contact points should be or how the network should work. The framework decision does not include any provisions on public-private cooperation either. This results in under-reporting to law enforcement and hampers effective investigation and prosecution.

3. Gaps in prevention

The information-sharing gaps affect public-private cooperation efforts on prevention, and criminals exploit the lack of awareness of the victims. All types of stakeholders (payers, payment services providers and payees) could benefit from prevention and awareness-raising.

According to the IA, all of the problem drivers identified above, except the long time needed to provide information on cross-border cooperation requests, can be attributed to the shortcomings of the current EU legal framework, rather than to a lack of implementation of existing EU rules (IA, p. 30). The framework decision has become partially obsolete, due mainly to technological developments, and this regulatory gap has not been sufficiently covered by more recent legislation. The evaluation presented in Annex 5 of the IA confirms this conclusion. The IA discusses the magnitude of the problem based on the European Central Bank (ECB) statistics from 2015 and 2016. The total value of card fraud using cards issued in the Single European Payment Area (SEPA) was estimated to amount to €1.44 billion in 2013. Fraud data on other means of non-cash payment at EU level is not available.[5] According to Europol,[6] well-structured and globally active organised crime groups dominate the criminal market for payment card fraud in the EU. Non-cash payment fraud provides income for organised crime and therefore facilitates criminal activities, such as terrorism, drug trafficking and trafficking in human beings. In addition, non-cash payment fraud hinders the development of the digital single market. A threat to security and an obstacle to the digital single market are thus the main consequences of the problem (IA, p. 18, 30). The effects of the problem on the various stakeholders – payers, payment services providers and payees – are also discussed (IA, pp. 12-17). Overall, the IA clearly defines the problem and acknowledges that its size is under-estimated due to only card fraud being considered (IA, p. 15, 34). This has to do with limited data

[4] For further information on the evaluation, see I. Kiendl Kristo, Council Decision 2001/413 on combating fraud and counterfeiting of non-cash means of payment, implementation appraisal, EPRS, European Parliament, November 2017.

[5] Fraud data exists only for card payments, cards being the most important payment instrument in terms of the number of transactions, according to the ECB (IA, p. 15 and figure 3 on p. 13). Assuming similar proportions to those in a recent UK study, Fraud the Facts 2016, the IA estimates the actual volume of fraud to be at least 25 % higher than card fraud. This excludes virtual currencies and mobile payments, for which no data could be located (IA, p. 15, footnote 42).

[6] Situation Report - Payment Card Fraud in the European Union, p. 3, Europol, 2012.

on the market size and the number of transactions involving virtual currencies, e-money and mobile payments, and lack of fraud data for these payment methods (IA, pp. 13-15).

Objectives of the legislative proposal

The IA sets two inter-related **general objectives,** which address the consequences of non-cash payment fraud and describe the ultimate goals of a proposed policy intervention (IA, p. 39):

1. to enhance security by reducing the attractiveness (i.e. reduce gains, increase risk) for organised crime groups of non-cash payment fraud as a source of income and therefore as an enabler of other criminal activities, including terrorism;
2. to support the digital single market, by reducing the negative impact on economic activity that non-cash payment fraud causes for the different stakeholders.

To address the problem drivers the IA sets three **specific objectives**:

1. to ensure that a clear, robust and technology neutral policy/legal framework is in place;
2. to eliminate operational obstacles that hamper investigation and prosecution;
3. to enhance prevention.

The link between the problem (sub-) drivers, specific and general objectives is presented in Table 2 of the IA and is rather straightforward (IA, p. 40). The IA sets only one **operational objective** for the preferred option: enhancing cross-border operational cooperation, which links to specific objective 2. This is quite limited and not fully in line with the Better Regulation Toolbox (Tool #16), which defines operational objectives in terms of the deliverables of specific policy actions. The IA also contains a list of indicators to monitor the achievement of the general, specific and operational objectives (IA, p. 79), which should ensure that the objectives are measurable, achievable and realistic. However, the objectives do not seem to be time-bound or specific enough and are therefore not entirely in line with the SMART criteria. The IA explains at length how the general and specific objectives are consistent with and complementary to those of other EU policies and legislation adopted since the framework decision (IA, pp. 40-46).

Range of options considered

Option 0: Baseline

All things being equal, the IA assumes that the annual growth rate demonstrated by ECB statistics would continue and the value of card fraud would double by 2020 compared to 2013. Quantitative estimates focus only on card fraud, since fraud data on other non-cash payments is not available. Among the qualitative considerations, the IA assumes that the value of monetary damage caused by cybercrime will continue to grow, emergence of new payment instruments will generate new opportunities for criminals and the cross-border nature of non-cash payment fraud will become even more relevant. Some existing EU instruments could contribute to reduce non-cash payment fraud to some extent, but since they do not fully address the problem drivers specific to non-cash payment fraud, the unresolved issues would develop as a result of separate initiatives in the Member States.

In addition to the baseline, the IA proposes **four regulatory options** with an increasing level of EU legislative action (IA, pp. 52-56):

- **A.** improve implementation of EU legislation and facilitate self-regulation for public-private cooperation;
- **B.** introduce a new legislative framework and facilitate self-regulation for public-private cooperation;
- **C.** same as option B but with provisions on encouraging reporting for public-private cooperation and new provisions on raising awareness;
- **D.** same as option C but with additional jurisdiction provisions complementing the European Investigation Order and injunction rules.[7]

[7] Orders granted by a court or an administrative body whereby someone is required to perform or to refrain from performing a specific action (IA, p. 56).

The measures these options contain and their link to the specific objectives are summarised in the table below:

<table>
<tr><th rowspan="2">Specific objectives</th><th colspan="4">Options</th></tr>
<tr><th>A</th><th>B</th><th>C</th><th>D</th></tr>
<tr><td>1. Ensure that a clear, robust and technology neutral policy/legal framework is in place</td><td rowspan="3">Implementation of existing EU law (e.g. the Framework Decision, the Payment Services Directive, the Directive on Attacks Against Information Systems), exchange of best practices, capacity building (guidelines, training courses, workshop events)</td><td colspan="3">Provisions in new directive including:
Technology neutral definitions, maintaining the part of the definition of payment instrument in the Framework Decision that specifies that the instrument should be secured, to encourage investments in security technologies
Preparatory acts covered as a separate offence and regardless of whether the fraudulent payment has occurred or whether it has generated financial losses for the victim; it also includes provisions criminalising identity theft as an aggravating circumstance
Minimum level of maximum penalties, coherent with the sanctions in related EU legislation, such as the Attacks Against Information Systems Directive
Jurisdiction (competence) rules as in the Attacks Against Information Systems Directive</td></tr>
<tr><td rowspan="2">2. Eliminate operational obstacles that hamper investigation and prosecution</td><td colspan="2">Provisions in new directive to facilitate effective cross-border cooperation, for example by strengthening and clarifying the role of dedicated contact points, encouraging Member States to share information with Europol, and collecting statistics on investigations and prosecutions of non-cash payment fraud offences</td><td>Provisions in new directive on complementing the European Investigation Order with measures adapted to non-cash payment fraud and adapting the rules on injunction for cooperation/evidence purposes</td></tr>
<tr><td rowspan="2">3. Enhance prevention</td><td>Facilitate self-regulation for public-private cooperation through exchange of information and a dedicated communication</td><td rowspan="2" colspan="2">Provisions in new directive on:
Requiring Member States to ensure appropriate reporting channels and remove (legal) obstacles that may hamper the exchange of information between private and public entities
Awareness-raising among potential victims (specific measures would be up to the Member States)</td></tr>
<tr><td>Address the lack of awareness through the implementation of existing EU law, exchange of best practices</td></tr>
</table>

Source: IA, author. Note: several measures correspond to more than one specific objective due to the underlying problem drivers – hence the cell alignment.

The policy options are cumulative (i.e. increasing level of EU legislative action). They have been formed by combining the policy measures retained after the mapping and analysis. Among the discarded measures were the following (IA, pp. 48-50):

- full harmonisation of level of penalties (minimum and maximum levels) is not feasible in EU criminal law, which can only introduce minimum rules on sanctions;
- creating an EU database on fraud data would bring about many different technical and legal challenges, such as data protection and retention issues;

- detailed definitions with a comprehensive list of payment instruments and forms of crime would risk becoming outdated in a short time;
- including preparatory acts as an aggravating circumstance without criminalising it would be less effective, since law enforcement would act only after the actual fraud occurred;
- adding new provisions protecting natural persons from identity theft and excluding legal persons would not properly cover an important group of victims;
- provisions on mandatory reporting to law-enforcement authorities would dramatically increase the administrative and financial costs borne by law enforcement agencies and the private sector.

The IA sets out the content of all options in a clear manner. As for option A, given that the problem definition states that most of the problem drivers can be attributed to the shortcomings of the current EU legal framework, rather than to a lack of implementation of existing EU rules, the usefulness of retaining this option for consideration is not immediately apparent. According to the IA, option C is the preferred option.

Scope of the Impact Assessment

The IA assesses the impacts of policy options in terms of coherence, effectiveness, efficiency, fundamental rights and EU added value (IA, pp. 57-66, pp. 161-184). It does not discuss the implications of a legal instrument (directive), nor does it contain any legal analysis of the effect of including preparatory acts regardless of whether the fraudulent payment has occurred or not. All assessments except efficiency (costs and benefits) are done qualitatively and detailed analyses are provided in Annex 4 of the IA. Quantification of costs and benefits, according to the IA, is limited by the lack of data, especially for the estimation of benefits. Social impacts (security) and economic impacts (digital single market) are part of the effectiveness assessment. The assessment of environmental impacts did not indicate any implications for the environment. An overview of qualitative scores for all options is provided in Table 11 of the IA (p. 67). Option D scored slightly better than C against several assessment criteria, such as social and economic impacts, but option C had a better overall qualitative score. Given the limitations of the quantitative assessment due to the lack of data, more weight was given to the qualitative assessment to decide on the preferred option (IA, p. 73). Limitations and assumptions are stated explicitly throughout the assessment. According to the IA (p. 59), the judgement and justifications of the qualitative scores were validated with focus group participants and external reviewers; however, the results of the validation are not reported in the IA report.

Subsidiarity / proportionality

The Commission proposal is based on Article 83(1) of the Treaty on the Functioning of the European Union (TFEU). The IA does not discuss the choice of legal instrument, but the proposal's explanatory memorandum states that in accordance with Article 83(1) TFEU, rules may only be established by means of a directive adopted in accordance with the ordinary legislative procedure. The IA includes a section on subsidiarity (p. 38) and demonstrates the need for EU action using two examples: a hypothetical case where as many as 10 Member States could be involved, causing substantial challenges in allocating jurisdiction (IA, p. 24) and a real 2013 case of counterfeiting cards affecting 27 countries (IA, p. 33). According to the IA, non-cash payment fraud has a significant cross-border dimension reinforced by its increasing digital/online component. Cross-border card transactions account for half of total card fraud (IA, p. 33). A subsidiarity and proportionality check is provided only for the preferred option (IA, pp. 75-76).

No reasoned opinions were submitted by national parliaments concerning the subsidiarity aspects of the proposal for which the deadline was 21 November 2017. Two national parliaments communicated their positions within the framework of political dialogue and information for exchange.[8] The Spanish Cortes Generales found the proposal in accordance with the principle of subsidiarity. The German Bundesrat was sceptical about the inclusion of 'virtual currencies' in the scope of criminal law protection, criminal liability long before an actual pecuniary loss has taken place and criminal liability for a mere attempt. Moreover, the

[8] See the Platform for EU Interparliamentary Exchange (IPEX).

Bundesrat deemed problematic the extension of the scope of criminal law in Article 11 establishing jurisdiction over offences causing damage in the Member State territory, including damage resulting from the theft of the identity of a person. Finally, the Bundesrat was mindful that the statistical requirements would significantly increase the burden on law enforcement.

Budgetary or public finance implications

According to its explanatory memorandum, the proposal has no immediate budgetary implications for the EU. The preferred option C would entail significant financial and administrative costs for national authorities. The IA estimates one-off costs of around €0.56 million for the Member States and €0.11 million for the EU, and annual costs of around €2.28 million for the Member States and €0.007 million for the EU (IA, p. 193). Due to the lack of data, the estimation of benefits was carried out mainly for the purposes of comparison of the options, rather than as an accurate estimate of the actual benefits (IA, p. 97).

SME test / Competitiveness

According to the IA, the proposed monitoring arrangements would not generate additional administrative burden (reporting obligations) for firms, including SMEs, beyond those already imposed by the reporting requirements on non-cash payment fraud data of Art. 96(6) of the Payment Services Directive 2015/2366/EU (IA, p. 78).

Simplification and other regulatory implications

The preferred option could bring some additional simplification benefits, thanks to the establishment of specific channels and tools for facilitating reporting, overall improved legal certainty of reporting and the lack of additional administrative burden on the private sector and citizens (IA, pp. 66, 180-181). The IA explains the coherence of the proposal's objectives with those of other EU policies on pp. 40-46 and additionally provides a coherence assessment for each policy measure and policy option in Annex 4.

Quality of data, research and analysis

The IA explains that the evaluation of the current situation was carried out 'back-to-back' (in parallel) with the impact assessment and delivered in the study 'Evaluation of the existing policy and legislative framework and preparation of impact assessment regarding possible options for a future EU initiative in combating fraud and counterfeiting of non-cash means of payment' (IA, p. 80). This study is referenced throughout the IA as the external expertise informing the assessment, but is not available online and therefore could not be verified for the purposes of this briefing. Besides the combined IA and evaluation study, the impact assessment work relied on the 2004 and 2006 Commission reports on the implementation of the framework decision, as well as other information sources that the author of this briefing could not retrieve online (IA, p. 81).[9] The IA openly states the limitations of its following components: the qualitative assessment of the impacts of the options (p. 58), the quantification of costs and benefits (pp. 62-64) and the evaluation (pp. 205-206). To mitigate the limitation of subjective judgements and justifications of the qualitative scores, they were validated with focus group participants and external reviewers (p. 59), but the results of this validation are not reported on in the IA. Besides, Annex 2 of the IA states that only seven stakeholders, representing EU institutions and bodies, private sector, public-private partnership, law enforcement and academia, attended the focus group (IA, p. 86). Such low attendance is rather surprising, considering that the qualitative assessment was given more weight when deciding on the preferred option (IA, p. 73). Overall, the quality of data and analysis of the IA seems to raise a number of questions, which could perhaps be answered if the external study were available online. Furthermore, a closer look at the evaluation methodology and the presentation of the findings reveals several inherent obstacles faced by the evaluators, such as the complex policy and legislative context of the framework

[9] Operational Action Plans 2014, 2015 and 2016 of the European multidisciplinary platform against criminal threats (EMPACT) sub-priority 'Payment Card Fraud' and the seventh cycle of mutual evaluation dedicated to preventing and combating cybercrime of the Council of the EU Working Party on General Matters including Evaluation (GENVAL).

decision, including interconnections with legal acts adopted thereafter, and the time that has elapsed since its adoption (16 years).

Stakeholder consultation

According to the IA, it is difficult to determine who is affected the most by non-cash payment fraud: whereas enablers (financial institutions, payment instruments, service providers) in general bear most of the liability, the payers (citizens and industries) are also significantly affected (IA, pp. 30-33). The stakeholders affected by the proposed initiative, according to the IA, are payers, enablers, payees (e.g. merchants, industries), law enforcement and judicial authorities, Member States and the EU (IA, pp. 94-95). Law enforcement and judicial authorities would face the greatest burden as a consequence of the initiative, due to a likely increase in the number of cases to be investigated, efforts to step up cross-border cooperation, an obligation for the Member States to gather statistics, and additional resources needed for private-public cooperation (IA, p. 95).

Three types of consultation activities were carried out in the context of the evaluation and the IA (pp. 83-93):

1. an open public consultation (12 weeks, practitioners and general public);
2. a targeted consultation organised by the European Commission (expert meetings with police authorities, judicial authorities and private sector, as well as academia, industries, consumers' organisations, financial regulators and private financial institutions);
3. a targeted consultation organised by the contractor (survey, interviews and a focus group with private sector, law enforcement agencies, victims' and consumers' organisations, national banking federations, EU institutions and bodies).

The open public consultation aimed to gather feedback on the current legal framework and the possible options to tackle existing issues. 33 practitioners from at least 13 Member States and 21 members of the general public from 9 Member States responded to the open public consultation. The synopsis of the contractors' consultation seems to focus predominantly on the evaluation of the current situation under the framework decision. The purpose of the focus group organised by the contractor was to present the main findings of the evaluation study, illustrate expected policy options and gather input on their impacts, but only 7 stakeholders attended it, compared to 88 stakeholders responding to the survey and 53 participating in the interviews. The synopsis report does not elaborate on the low attendance rate of the focus group and its representativeness. Although the IA does mention that one of the expert meetings organised by the Commission focused on gathering experts' views on the possible solutions to the problems identified, it does not report anything about the results of this meeting, the preferences of stakeholders or their views on the options. Therefore, it is not clear what the stakeholders' views were on the retained or discarded measures and options. Overall, the IA provides a rather inconsistent synopsis of all three consultations in Annex 2, while stakeholders' contributions are not available online. This leaves a generally poor impression of the stakeholder consultation.

Monitoring and evaluation

The IA proposes that the Commission submit a report assessing the extent to which the Member States have taken the necessary measures in order to comply with the legislative act two years after the deadline for implementation. The evaluation of the impacts of the legislation is proposed six years after the deadline for implementation. The IA contains a list of indicators to monitor the achievement of the general, specific and operational objectives (IA, p. 79). 8 out of 11 proposed indicators rely on existing data sources (e.g. ECB, Eurobarometer) and the remaining 3 indicators represent a requirement for the Member States to collect annual national statistics on non-cash payment fraud crimes:

- the ratio between fraud volume and law enforcement action;
- the number of structured public-private cooperation mechanisms established and number of entities involved;
- the number of national contact points set up in accordance with the preferred policy option.

Commission Regulatory Scrutiny Board

The Regulatory Scrutiny Board (RSB) issued a positive opinion on the draft of the IA on 12 July 2017. The Board acknowledged the efforts to quantify costs and benefits and recommended to improve the report with respect to the broader policy context and the impact on growth. The latter, according to the RSB, was an indirect result of enhanced trust in the single digital market and therefore overstated (the final IA does not set a growth objective). Further considerations of the Board were related to the evaluation, the logic behind the options and the difference between them, improvements to the impacts section and the overall presentation of the report. The IA does not contain a section explaining the modifications made to the report following the RSB recommendations, which is not in line with Better Regulation Toolbox (Tool #12), but overall it seems to have responded to a great extent to the comments expressed in the RSB opinion.

Coherence between the Commission's legislative proposal and IA

According to its explanatory memorandum, the legislative proposal appears to follow the recommendations of the IA insofar as the preferred option C is the basis for the proposal.

Conclusions

The IA presents the problem of non-cash payment fraud in a coherent and clear manner. The link between the problem (sub-) drivers, specific and general objectives of the proposal is rather straightforward. The objectives could be more specific and time-bound, however, to bring them in line with the SMART criteria. The IA sets out the content of all options in a clear manner. However, the quality of data, analysis and stakeholder consultation leaves an overall poor impression, partly because the combined IA and evaluation study, which is the external expertise informing the assessment, is not available online and therefore impossible to verify. For instance, according to the IA, the qualitative scores were validated with the focus group participants and external reviewers; however, the results of the validations are not reported in the IA report and only seven stakeholders attended the focus group. Such low attendance is rather surprising, considering that the qualitative assessment was given particular weight when deciding on the preferred option. The IA provides a rather inconsistent synopsis of the three consultation processes and the stakeholders' contributions are not available online. The IA does not make clear what the stakeholders' views were on the retained or discarded measures and options. Making the study accessible online could perhaps provide the information needed to understand the logic behind the assessment, the stakeholder consultation and the choice of the preferred option.

To contact the Ex-Ante Impact Assessment Unit, please e-mail: EPRS-ImpactAssessment@europarl.europa.eu

Manuscript completed in December 2017.