EUROPEAN
COMMISSION

Brussels, 13.9.2017
COM(2017) 489 final

2017/0226 (COD)

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

{SWD(2017) 298 final}
{SWD(2017) 299 final}

TABLE OF CONTENTS

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

1.1. Reasons for and objectives of the proposal

The current EU legislation that provides common minimum rules to criminalise non-cash payment fraud is Council Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment[1].

The European Agenda on Security[2] acknowledges that the Framework Decision no longer reflects today's realities and insufficiently addresses new challenges and technological developments such as virtual currencies and mobile payments.

In 2013, fraud using cards issued in the Single European Payment Area (SEPA) reached EUR 1.44 billion, representing growth of 8 % on the previous year. Although fraud data exists only for card payments, cards are the most important non-cash payment instrument in the EU in terms of number of transactions[3].

It is important to deal effectively with non-cash payment fraud as it represents a threat to security. Non-cash payment fraud provides income for organised crime and therefore enables other criminal activities such as terrorism, drug trafficking and trafficking in human beings. In particular, according to Europol, non-cash payment fraud income is used to finance:

- Travel:
  - flights: the experience gained from conducting the Global Airline Action Day[4] operations from 2014 to 2016 indicates a clear link between non-cash payment fraud, airline ticketing fraud and other serious and organised crimes, including terrorism. Some of the people travelling on fraudulently obtained tickets were known or suspected to be involved in other offences;
  - other travel fraud (i.e. selling and travelling on tickets that have been obtained fraudulently). The main way to purchase illegal tickets was through the use of compromised credit cards. Other methods included the use of compromised loyalty point accounts, phishing travel agencies and voucher fraud. In addition to criminals, those travelling on fraudulently obtained tickets included victims of trafficking and people acting as 'money mules'[5].
- Accommodation: law enforcement also reports that non-cash payment fraud is also used to facilitate other crimes that require temporary accommodation such as trafficking in human beings, illegal immigration and drug trafficking.

Europol also reported that the criminal market for payment card fraud in the EU is dominated by well-structured and globally active organised crime groups[6].

---

1 Official Journal L 149, 02.06.2001 p.1.

2 Commission communication *A Digital Single Market Strategy for Europe*, COM(2015) 192 final.

3 European Central Bank, *Fourth report on card fraud*, July 2015 (latest data available).

4 More details here.

5 The term 'acting as a money mule' indicates a person who transfers proceeds of crime between different countries. Money mules receive the proceeds into their account; they are then asked to withdraw them and wire the money to a different account, often overseas, keeping some of the money for themselves.

6 Europol, *Situation Report: Payment Card Fraud in the European Union*, 2012.

In addition, non-cash payment fraud hinders the development of the digital single market in two ways:

- it causes important direct economic losses, as the estimated level of card fraud of EUR 1.44 billion mentioned above indicates. For example, the airlines lose around USD 1 billion per year globally in card fraud[7];
- it reduces consumers' trust, which may result in reduced economic activity and limited engagement in the digital single market. According to the most recent Eurobarometer on Cyber Security[8], the vast majority of Internet users (85 %) feel that the risk of becoming a victim of cybercrime is increasing. In addition, 42 % of users are worried about the security of online payments. Because of security concerns, 12 % are less likely to engage in digital transactions such as online banking.

An evaluation of the current EU legislative framework[9] identified three problems that are driving the current situation concerning non-cash payment fraud in the EU:

1. Some crimes cannot be **effectively investigated and prosecuted** under the current legal framework.
2. Some crimes cannot be effectively investigated and prosecuted due to operational obstacles.
3. Criminals take advantage of gaps in **prevention** to commit fraud.

This proposal has three specific objectives that address the problems identified:

1. Ensure that a clear, robust and **technology neutral** policy/legal framework is in place.
2. Eliminate **operational obstacles** that hamper investigation and prosecution.
3. Enhance **prevention.**

1.2. Need to implement relevant international standards and obligations and address fraud and counterfeiting on non-cash means of payment in an effective manner

The Council of Europe Convention on Cybercrime (Budapest Convention)[10], in its Title 2 covering computer-related offences, requires the Parties to the Convention to establish computer-related forgery (Article 7) and computer-related fraud (Article 8) as criminal offences under their respective domestic laws. The current Framework Decision complies with these provisions. Revising the present rules will enhance cooperation among police and judicial authorities and between law enforcement and private entities even further, therefore contributing to meeting the overall objectives of the Convention, remaining consistent with its relevant provisions.

1.3. Consistency with existing policy provisions in the policy area

The objectives of this proposal are consistent with the following policy and legislative provisions in the area of criminal law:

---

7 IATA, 2015.

8 European Commission, *Special Eurobarometer 423 — Cyber Security*, February 2015.

9 Commission Staff Working Document – Impact Assessment accompanying the Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment, SWD(2017)298.

10 Council of Europe Convention on Cybercrime (ETS No 185).

1. Pan-European **cooperation mechanisms in criminal matters** that facilitate coordination of investigation and prosecution (procedural criminal law):

- Council Framework Decision 2002/584/JHA on the European Arrest Warrant and the surrender procedures between Member States[11];
- Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[12];
- Directive 2014/41/EU regarding the European Investigation Order in criminal matters[13];
- Council Framework Decision 2005/214/JHA on the application of the principle of mutual recognition to financial penalties[14];
- Council Framework Decision 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings[15];
- Council Framework Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from the criminal record between Member States[16];
- Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime[17];
- Regulation (EU) 2016/794 on Europol[18];
- Council Decision 2002/187/JHA setting up Eurojust[19];
- Council conclusions on improving criminal justice in cyberspace[20].

As a principle, this proposal does not introduce provisions specific to non-cash payment fraud that would deviate from these broader instruments, to avoid fragmentation which could complicate the transposition and implementation by Member States. The only exception is Directive 2012/29/EU on the rights, support and protection of victims, which this proposal complements.

---

11 2002/584/JHA Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.

12 Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

13 Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters

14 Council Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties.

15 Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings.

16 Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States.

17 Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA.

18 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

19 Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime.

20 Council conclusions of 6 June 2016 on improving criminal justice in cyberspace.

2. Legal acts that **criminalise conduct** related to fraud and counterfeiting of non-cash means of payment (substantive criminal law):

- Directive 2013/40/EU on attacks against information systems[21]:
  - this proposal is complementary to Directive 2013/40, by addressing a different aspect of cybercrime[22]. The two instruments correspond to different sets of provisions of the Council of Europe Budapest Convention on Cybercrime[23], which represents the international legal framework of reference for the EU[24];
  - this proposal is also consistent with Directive 2013/40, as it is based on a similar approach regarding specific issues such jurisdiction or defining minimum levels of maximum penalties.
- Directive 2014/62/EU on the protection of the euro and other currencies against counterfeiting by criminal law[25]:
  - this proposal is complementary to Directive 2014/62/EU as it covers counterfeiting of non-cash payment instruments, while Directive 2014/62/EU covers the counterfeiting of cash;
  - it is also consistent with Directive 2014/62/EU as it uses the same approach on some provisions such as on investigative tools.
- Directive 2017/541/EU on combating terrorism:
  - this proposal is complementary to Directive 2017/541/EU as it aims to reduce the overall amount of funds obtained from non-cash payment fraud, most of which go to organised crime groups to commit serious crimes, including terrorism.
- The proposal for a Directive on countering money laundering by criminal law:
  - this proposal and the proposal for a Directive on countering money laundering by criminal law are complementary as the latter provides the necessary legal framework to counter the laundering of criminal proceeds generated by non-cash payment fraud ('money mules') as a predicate offence.

---

21 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

22 The EU cybersecurity strategy indicates that 'cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)'.

23 Council of Europe Convention on Cybercrime (ETS No 185). Directive 2013/40 corresponds to Articles 2 to 6 of the Convention, whereas a new initiative would correspond to Articles 7 and 8 of the Convention.

24 Commission and the High Representative of the European Union for Foreign Affairs and Security Policy — Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

25 Directive 2014/62/EU of the European Parliament and of the Council of 15 May 2014 on the protection of the euro and other currencies against counterfeiting by criminal law, and replacing Council Framework Decision 2000/383/JHA.

1.4. Consistency with other EU policies

This proposal is consistent with the EU Agenda on Security and the EU Cybersecurity Strategy as these have enhancing security as a main objective.

In addition, this proposal is consistent with the Digital Single Market Strategy which seeks to strengthen user confidence in the digital marketplace, another main objective of the proposal. In the context of the Digital Single Market Strategy, several legal instruments exist to facilitate secure payments across the EU, and with which this proposal is also consistent:

- Revised Payment Services Directive (PSD2)[26] contains a number of measures which will enhance the security requirements for electronic payments and will provide a legal and supervisory framework for emerging participants in the payment market.
- Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[27], (the fourth Anti-Money Laundering Directive) covers the situation where criminals abuse non-cash payment instruments with a view to concealing their activities. This proposal complements it by addressing the situation where the non-cash payment instruments have been, for instance, unlawfully appropriated, counterfeited or falsified by the criminals.
- Proposal for a Directive amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[28], from which this proposal takes the same definition of virtual currencies. If this definition changes during the adoption process of the former proposal, the definition in this proposal should be aligned accordingly.
- Other relevant legal acts include Regulation (EU) 2015/847 on information accompanying transfers of funds[29]; Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market[30]; Regulation (EU) 2012/260 establishing technical and business requirements for credit transfers and direct debits in euro[31]; and Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)[32].

---

26 Directive (EU) 2015/2366 of the European Parliament and of The Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

27 Directive 2015/849/EU of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

28 Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC.

29 Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

30 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

31 Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009.

32 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

In general, these legal acts help put in place stronger preventive measures. This proposal complements them by adding measures to impose sanctions on criminal activity and to enable prosecution where prevention has failed.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

2.1. Legal basis

The legal basis for EU action is Article 83(1) of the Treaty on the Functioning of the European Union, which explicitly mentions **counterfeiting of means of payment, computer crime and organised crime** as areas of particularly serious crimes with a cross-border dimension:

> *'The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a **cross-border dimension** resulting from the nature or impact of such offences or from a special need to combat them on a common basis.*
>
> *These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, **counterfeiting of means of payment, computer crime and organised crime**…'*

2.2. Variable geometry

The Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment applies to all Member States.

In accordance with Protocol 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice annexed to the Treaties, the United Kingdom and Ireland may decide to take part in the adoption of this proposal. They also have this option after adoption of the proposal.

Since the United Kingdom notified on 29 March 2017 its intention to leave the Union, pursuant to Article 50 of the Treaty on European Union (TEU), the Treaties will cease to apply to the United Kingdom from the date of the entry into force of the withdrawal agreement or, failing that, two years after the notification, unless the European Council, in agreement with the United Kingdom, decides to extend that period. As a consequence, and without prejudice to any provisions of the withdrawal agreement, this above-mentioned description of the participation of the UK in this proposal only applies until the United Kingdom ceases to be a Member State.

Under Protocol 22 on the position of Denmark, Denmark does not take part in the Council's adoption of the measures pursuant to Title V of the TFEU (with the exception of visa policy). Therefore, under the arrangements currently in force, Denmark does not take part in the adoption of this proposal and will not be bound by it.

2.3. Subsidiarity

Non-cash payment fraud has a very important cross-border dimension both within the EU and beyond. A typical case may involve the skimming (copying) of card data in an EU country, the creation of a counterfeit card using that data, and the cashing out with the counterfeit card outside the EU to circumvent the high security standards. Increasingly, these crimes are moving entirely online.

Therefore, the objective of effectively combating such crimes cannot be sufficiently achieved by Member States acting alone or in an uncoordinated way:

- these crimes create situations where the victim, the perpetrator and the evidence can all be under different national legal frameworks within the EU and beyond. As a result, it can be very time consuming and challenging for single countries to effectively counter these criminal activities without common minimum rules;
- the need for EU action has already been acknowledged through the creation of the existing EU legislation on combating fraud and counterfeiting of non-cash means of payment (the Framework Decision);
- the need for EU intervention is also reflected in the current initiatives to coordinate Member States measures in this field at EU level, such as a dedicated Europol team working on payment fraud[33] and the EMPACT Policy Cycle priority on operational cooperation against non-cash payment fraud[34]. The added value of these initiatives in helping Member States combating these crimes was acknowledged multiple times in the stakeholder consultation during this proposal's preparation, in particular during the expert meetings.

Another added value of EU action is to facilitate cooperation with non-EU countries given that the international dimension of non-cash payment fraud frequently goes beyond EU borders. The existence of minimum common rules in the EU can also inspire effective legislative solutions in non-EU countries thereby facilitating cross-border cooperation globally.

2.4. Proportionality

In accordance with the principle of proportionality, as set out in Article 5(4) TEU, the proposed new Directive is limited to what is necessary and proportionate to implement international standards and adapt existing legislation on offences in this area to new threats. Measures related to the use of investigative tools and information exchange are included only to the extent needed for the proposed criminal law framework to function effectively.

The proposal defines the scope of the criminal offences to cover all relevant conduct while limiting it to what is necessary and proportionate.

2.5. Choice of instrument

In accordance with Article 83(1) TFEU minimum rules concerning the definition of criminal offences and sanctions in the area of serious crime with a cross-border dimension, including counterfeiting of means of payment and computer crime, may only be established by means of a Directive of the European Parliament and the Council adopted in accordance with the ordinary legislative procedure.

[33] See Europol's website.
[34] More information here.

3. RESULTS OF EX POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

3.1. Ex-post evaluations/fitness checks of existing legislation

The Commission carried out an evaluation[35] of the current EU legislative framework together with the impact assessment accompanying this proposal (see corresponding Commission Staff Working Document for more information).

The evaluation detected three problem drivers, each with a number of sub-drivers:

Drivers	Sub-drivers
1. Some crimes cannot be **effectively investigated and prosecuted** under the current **legal framework.**	a. Certain crimes cannot be prosecuted effectively because offences committed with certain payment instruments (in particular **non-corporeal**) are criminalised differently in Member States or not criminalised. b. **Preparatory acts** for non-cash payment fraud cannot be prosecuted effectively because they are criminalised differently in Member States or not criminalised. c. Cross-border investigations can be hampered because the same offences are sanctioned with different **levels of penalties** across Member States. d. Deficiencies in allocating **jurisdiction** can hinder effective cross-border investigation and prosecution.
2. Some crimes cannot be **effectively investigated and prosecuted** due to **operational obstacles.**	a. It can take too much time to provide information in **cross-border cooperation** requests, hampering investigation and prosecution. b. Under-reporting to law enforcement due to constraints in **public-private cooperation** hampers effective investigations and prosecutions.
3. Criminals take advantage of gaps in **prevention** to commit fraud.	a. **Information sharing** gaps in **public-private cooperation** hamper prevention. b. Criminals exploit the **lack of awareness** of victims.

The problem drivers indicate that the issue at hand is mostly a **regulatory failure,** where the current EU legislative framework (the Framework Decision) has become partially obsolete, due mainly **to technological developments.** The evaluation indicated that this regulatory gap has not been sufficiently covered by more recent legislation.

3.2. Stakeholder consultations

Consultation activities:

Three types of consultation activities were carried out: open public consultation, targeted consultation organised by the European Commission and targeted consultation organised by a contractor:

1. Open public consultation

[35] Commission Staff Working Document – Impact Assessment accompanying the Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment, SWD(2017)298.

The European Commission launched an open public consultation on 1 March 2017, which aimed to gather feedback from the public at large on the problem definition, the relevance and effectiveness of the current legal framework in the field of non-cash payment fraud, as well as options, and their possible impacts to tackle existing issues. The consultation closed after 12 weeks, on 24 May 2017.

33 practitioners and 21 members of the general public answered the consultation's questionnaires. Four practitioners provided additional input through written contributions. Practitioners included:

- private companies (private sector);
- international or national public authorities (law enforcement agencies, judicial authorities and EU institutions and bodies);
- trade, business or professional associations (e.g. national banking federations);
- non-governmental organisations, platforms or networks;
- professional consultancies, law firms, self-employed consultants.

2. Targeted consultation organised by the European Commission:

- large expert meetings with representatives from police and judicial authorities from all EU countries (selected by Member States) and experts from the private sector (financial institutions, payment service providers, merchants, card schemes);
- various meetings with experts and stakeholders from academia, law enforcement agencies, virtual currencies industries, representatives of consumer organisations, representatives of private financial institutions and representatives of financial regulators.

3. Targeted consultation organised by a contractor:

A contractor organised targeted consultations that included online surveys and interviews. The preliminary results were presented to a validation focus group which then provided feedback and verified the consultation's results.

Overall, 125 stakeholders were involved from 25 Member States.

Main results:

- Dimension of crime:

  Costs related to non-cash payment fraud were generally perceived as high and were expected to increase in the coming years. Stakeholders from all categories faced difficulties when asked to quantify the criminal phenomenon. Statistics are rare and not always accessible. Some of them, however, provided case-based evidence implying the significance of certain types of non-cash payment fraud.

- Criminal law framework:

  Most stakeholders considered the current EU legal framework only partially relevant to current security needs, especially concerning the definition of payment instruments and criminal offences. Some confirmed that national legal frameworks would need to be amended.

- Procedural criminal law:

  Despite the existing legal framework, the current level of cooperation between Member States for investigations and prosecutions was perceived to be only partially satisfactory. Europol's support in facilitating cross-border cooperation was widely acknowledged.

- Reporting to law enforcement authorities:

  Views on reporting to law enforcement authorities differed: some were satisfied with the current level of reporting, while others believed it should be improved. The different categories of stakeholders agreed that future policy options on reporting need to be balanced with the actual capacities of law enforcement authorities to follow-up on cases.

- Public-private cooperation:

  Stakeholders felt that cooperation between public and private entities was beneficial overall and agreed that it should be encouraged to better tackle non-cash payment fraud, particularly when it comes to prevention.

  Most of the stakeholders considered that public-private cooperation should be improved to combat non-cash payment fraud. Private sector representatives appeared to be the most dissatisfied. They perceive the main obstacles to cooperation to include, for instance, limitations in the possibility to share information with law enforcement authorities and in related tools used to enable the exchange.

  The vast majority of stakeholders agreed that in order to investigate and prosecute criminals, financial institutions should be allowed to spontaneously share some of the victim's personal information with the national police or the police of another EU country (e.g. name, bank account, address, etc.).

  Poor cooperation between private and public authorities was also mentioned by several stakeholders as an obstacle to fighting non-cash payment fraud.

  Legislation, misalignment of priorities and lack of trust, together with practical and organisational issues, were seen by private enterprises, public authorities, trade, business and professional associations as obstacles to successful cooperation between public authorities and private entities when participants are based in different EU countries. A lack of appropriate technology (e.g. channel of communications) was mentioned as an obstacle by private enterprises and public authorities.

- Victims' rights:

  Stakeholders stressed the importance of protecting victims of fraud. Some of them felt that victims are not sufficiently protected, although initiatives taken at Member State level to protect them are appreciated. Victims associations have developed good cooperation mechanisms with law enforcement authorities. Several stakeholders considered it necessary to better protect victims against identity theft, which they perceived as affecting natural persons as well as legal persons. Therefore victims should be protected regardless of their legal nature.

3.3. Impact assessment

In accordance with the Commission's Better Regulation Guidelines[36], the Commission conducted an impact assessment[37] to assess the need for a legislative proposal.

The impact assessment was presented to and discussed with the Regulatory Scrutiny Board (RSB) on 12 July 2017. The Board acknowledged the efforts to quantify costs and benefits. It gave a positive opinion[38], with a recommendation to further improve the report with respect to the following aspects:

1. The report did not sufficiently explain the policy context, including the relationship with and complementarity of existing and envisaged judicial and pan-European cooperation mechanisms.
2. The objective of the initiative related to growth seemed overstated.

The impact assessment report was revised taking into account the recommendations of the Board in its positive opinion.

After mapping the possible policy measures to tackle each of the problems identified in the evaluation, and analysing which measures to retain and which to discard, the measures were grouped into policy options. Each policy option was built to address all the problems identified. The various policy options considered were cumulative, i.e. with an increasing level of EU legislative action. Given that the problem at hand is basically a **regulatory failure**, it was important to lay out the full range of regulatory tools to determine the most proportionate EU response.

The different options considered were:

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

Option C was the preferred option, both qualitatively and in terms of costs and benefits.

In terms of benefits, the preferred option would pave the way towards more effective and efficient law enforcement action against non-cash payment fraud, through a more coherent application of rules across the EU, better cross-border cooperation, and stronger public-private cooperation and exchange of information. The initiative would also foster trust in the digital single market, by strengthening security.

In terms of costs, the costs of creating and implementing a new initiative for Member States are estimated to be around EUR 561 000 (one-off). Continuous costs for implementation and

---

36 More information on Better Regulation Guidelines is available here.

37 Commission Staff Working Document – Impact Assessment accompanying the Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment, SWD(2017)298.

38 European Commission Regulatory Scrutiny Board – Opinion on the Impact Assessment – Combating fraud and counterfeiting of non-cash means of payment, SEC(2017)390.

enforcement for Member States are estimated to be around EUR 2 285 140 per year (total all Member States).

As no mandatory rules on reporting are envisaged by the proposal, there should be no impact with regard to additional costs for businesses, including SMEs. The other provisions that would be included in the proposal also do not affect SMEs.

Overall, the cumulative impact of the proposed measures on administrative and financial costs is expected to be higher than the current levels, as the numbers of cases to be investigated would put a strain on law enforcement resources in this area, which would need to be increased. The main reasons for that are:

- a broader definition of the means of payment and additional offences to be tackled (preparatory acts) is likely to increase the number of cases that police and judicial authorities are responsible for;
- additional resources would be required to step up cross-border cooperation;
- an obligation for Member States to gather statistics would create an additional administrative burden.

On the other hand, establishing a clear legal framework to tackle enablers for non-cash payment fraud would provide a chance for detecting, prosecuting and sanctioning fraud-related activities earlier on. Moreover, while enhancing public-private cooperation has a cost in terms of resources, the return on investment in terms of effectiveness and efficiency of law enforcement action is immediate.

3.4. Regulatory fitness and simplification

Qualitatively, this proposal has simplification potential in a few areas, e.g.:

- further approximation of national criminal law frameworks (e.g. by providing common definitions and a common minimum level of sanctions for the maximum penalties) would simplify and facilitate cooperation between national law enforcement agencies investigating and prosecuting cross-border cases;
- in particular, clearer rules on jurisdiction, a reinforced stronger role for national contact points and the sharing of data and information between national police authorities and with Europol could further simplify the procedures and practices for cooperation.

It is not possible to quantify the simplification potential due to a lack of data (and in some cases the impossibility to isolate the effects of the Framework Decision).

Overall, the regulatory fitness potential of this initiative is very limited:

1. Firstly, the 2001 Framework Decision is already a relatively simple legal act with limited potential to be further simplified.
2. Secondly, this initiative aims to increase security by addressing the current gaps. This would normally entail more administrative costs to investigate and prosecute crimes that are not currently covered, rather than significant savings that would result from simplifying cross-border cooperation.
3. Thirdly, the initiative does not aim to impose additional legal obligations on businesses and citizens. It requests Member States to encourage and facilitate reporting through appropriate channels (rather than imposing mandatory reporting),

in line with other EU instruments such as Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography (Article 16(2)).

3.5. Fundamental rights

The proposal includes provisions to adapt the legal framework on combating fraud and counterfeiting of non-cash means of payment to new and emerging threats and to regulate forms of non-cash payment fraud not currently covered.

The final objective of these measures is to protect the rights of victims and potential victims. Establishing a clear legal framework for law enforcement and judicial authorities to act upon criminal activities directly affecting the personal data of the victims, including the criminalisation of preparatory acts, may in particular have a positive impact on the protection of victims' and potential victims' right to privacy and right to protection of personal data.

At the same time, all measures as provided for in this proposal respect fundamental rights and freedoms as recognised by the Charter of Fundamental Rights of the European Union, and must be implemented accordingly. Any limitation on the exercise of such fundamental rights and freedoms is subject to the conditions set out in Article 52(1) of the Charter, namely that they be subject to the principle of proportionality with respect to the legitimate aims of genuinely meeting objectives of general interest recognised by the Union and protecting the rights and freedoms of others. Limitations must be provided for by law and respect the essence of the rights and freedoms set out in the Charter.

A variety of fundamental rights and freedoms enshrined in the Charter have been taken into account in this respect, including: the right to liberty and security; the respect for private and family life; the freedom to choose an occupation and right to engage in work; the freedom to conduct a business; the right to property; the right to an effective remedy and to a fair trial; the presumption of innocence and right of defence; the principles of the legality and proportionality of criminal offences and penalties as well as the right not to be tried or punished twice in criminal proceedings for the same criminal offence.

In particular, this proposal respects the principle that criminal offences and penalties must be set out in law and be proportionate. It limits the scope of the offences to what is necessary to allow effective prosecution of acts that pose a particular threat to security and it introduces minimum rules on the level of sanctions in accordance with the principle of proportionality, having regard to the nature of the offence.

This proposal is also designed to ensure that data of persons suspected of the offences listed by this Directive be handled in accordance with the fundamental right to protection of personal data and existing applicable legislation, including in the context of public-private cooperation.

4. BUDGETARY IMPLICATIONS

This proposal has no immediate budgetary implications for the EU.

5. OTHER ELEMENTS

5.1. Implementation plans and monitoring, evaluation and reporting arrangements

The Commission will monitor the implementation of the Directive using information provided by the Member States on the measures taken to bring into force the laws, regulations and administrative provisions necessary to comply with the Directive.

After two years following the deadline for implementing this Directive, the Commission will submit a report to the European Parliament and to the Council assessing the extent to which the Member States have taken the necessary measures to comply with this Directive.

In addition, the Commission will conduct an evaluation of the impacts of this Directive six years after the deadline for its implementation, to ensure that there is a sufficiently long period to evaluate the effects of the initiative after it has been fully implemented across all Member States.

5.2. Explanatory documents

No explanatory documents on the transposition are considered necessary.

6. LEGAL ELEMENTS OF THE PROPOSAL

6.1. Summary of the proposed action

This proposal, while repealing Framework Decision 2001/413/JHA, updates most of its current provisions and is consistent with the findings of the evaluation and the impact assessment (e.g. with regard to the preferred option).

The following table shows how this proposal corresponds with the Framework Decision and indicates which articles are new and which ones have been updated from the Framework Decision:

	DIRECTIVE		FRAMEWORK DECISION		Comments
	Article	**Recital**	**Article**	**Recital**	
I. Subject matter and definitions	1. Subject matter	1-6	None	1-7	New
	2. Definitions	7-8	1. Definitions	10	Updated
II. Offences	3. Fraudulent use of payment instruments	9	2. Offences related to payment instruments	8-10	
	4. Offences preparatory to the fraudulent use of payment instruments				
	5. Offences related to information systems		3. Offences related to computers		
	6. Tools used for committing offences		4. Offences related to specifically adapted devices		
	7. Incitement, aiding and abetting and attempt		5. Participation, instigation and attempt		
	8. Penalties for natural persons	10-11	6. Penalties	9	
	9. Liability of legal persons	None	7. Liability of legal persons	None	
	10. Sanctions for legal persons		8. Sanctions for legal persons		
III. Jurisdiction and investigation	11. Jurisdiction	12-14	9. Jurisdiction; 10. Extradition and prosecution	11	
	12. Effective investigations	15	None	None	New
IV. Exchange of information and reporting of crime	13. Exchange of information	16-18	11. Cooperation between Member States; 12. Exchange of information	11	Updated
	14. Reporting of crime	19	None	None	New
V. Assistance and support to victims and prevention	15. Assistance and support to victims	20-22	None		
	16. Prevention	23	None		
VI. Final provisions	17. Monitoring and statistics	24	None		
	18. Replacement of Framework Decision	25	None		
	19. Transposition	None	14. Implementation [14(1)]		Updated
	20. Evaluation and reporting		14. Implementation [14(2)]		
	21. Entry into force		15. Entry into force		
	None	26-29	13. Territorial application		Deleted

Specifically, this proposal:

- defines the payment instruments in a more encompassing and robust way which also includes non-corporeal payment instruments, as well as digital mediums of exchange;
- makes it a self-standing offence, aside from using such instruments, to possess, sell, procure for use, import, distribute or otherwise make available a stolen or otherwise unlawfully appropriated counterfeited or falsified payment instrument;
- expands the scope of the offences related to information systems to include all payment transactions, including transactions through digital exchange mediums;
- introduces rules on the level of penalties, in particular setting a minimum level for maximum penalties;
- includes aggravated offences for:
- situations where the criminal acts are committed within the framework of a criminal organisation, as defined in Framework Decision 2008/841/JHA, irrespective of the penalty provided for therein;
- situations where the criminal act causes considerable aggregate damage or provides considerable economic benefit for the offenders. This aims to address the cases of high-volume, low individual losses, in particular in card-not-present fraud.
- clarifies the scope of the jurisdiction regarding the offences referred to in the proposal by ensuring that Member States have jurisdiction in cases either where the offence has been committed using an information system located within the territory of the Member State while the offender may be located outside of it or if the offender is located within the territory of the Member State but the information system may be located outside of it;
- clarifies the scope of the jurisdiction regarding the effects of the offence by ensuring that Member States are able to exercise jurisdiction if the offence causes damage in their territory, including damage resulting from the theft of a person's identity;
- introduces measures to improve Union-wide criminal justice cooperation by strengthening the existing structure and use of the operational contact points;
- enhances the conditions for victims and private entities to report crime;
- addresses the need to provide statistical data on fraud and counterfeiting of non-cash means of payment by obliging Member States to ensure that a suitable system is in place for recording, producing and providing statistical data on the offences referred to in the proposed directive;
- provides for victims to have access to information about their rights and about available assistance and support, regardless of whether their country of residence is different from the one of the perpetrator of the fraud or where the criminal investigations take place.

6.2. Detailed explanation of the specific provisions of the proposal

Article 1: Subject matter — this Article sets out the scope and purpose of the proposal.

Article 2: Definitions — this Article sets out definitions which apply throughout the instrument. Article 2 includes the same definition of virtual currencies as in the Commission Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC.[39] If this definition changes during the adoption process of the above proposal, the definition of virtual currencies in this Article should be aligned accordingly.

Article 3: Fraudulent use of payment instruments — this Article lists the offences relating to criminal conduct that directly and immediately constitutes fraud, namely fraudulent use of payment instruments, including both stolen and counterfeited instruments. The offences apply to all payment instruments, whether corporeal or not, so this also covers fraud committed using stolen or falsified payment credentials or other records enabling or used to initiate a payment order or other monetary transfer, including transfers of virtual currency.

Article 4: Offences preparatory to the fraudulent use of payment instruments — this Article sets out offences relating to criminal conduct that, while not immediately constituting the actual fraud leading to loss of property, are committed in preparation for fraud. These include the theft or counterfeiting of a payment instrument and various acts involved in trafficking of those stolen or counterfeited instruments. It includes possession, distribution or making them available to be used fraudulently, including cases where the offender is aware of the possibility of fraudulent use (*dolus eventualis*). Like Article 3, it covers all offences involving payment instruments, whether they are corporeal or not, and therefore also applies to behaviour such as trade in stolen credentials ('carding') and phishing[40].

Article 5: Offences related to information systems — this Article sets out offences relating to information systems to be criminalised by Member States. The list contains elements that distinguish the offences from illegal system interference or illegal data interference under Directive 2013/40/EU, such as the transfer of monetary value to procure unlawful gain. This provision has been included with a view to criminalising conduct such as hacking a victim's computer or a device in order to re-direct the victim's traffic to a forged online banking website, thus causing the victim to make a payment to a bank account controlled by the offender (or 'money mules')[41]. It also covers other forms of criminal conduct, such as pharming[42], which exploit information systems to make an unlawful gain for the perpetrator or another person.

Article 6: Tools used for committing offences — this Article sets out offences relating to tools used for committing offences referred to in Article 4(a) and 4(b) and Article 5, to be

---

39 COM(2016) 450 final.

40 Phishing is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Most commonly, an email that appears to be from a well-known and trusted company is sent to a large list of email addresses. The email may direct the recipient to a spoofed Web page, where he or she is asked for personal information.

41 The term "acting as a money mule" indicates a person who transfers proceeds of crime between different countries. Money mules receive the proceeds into their account; they are then asked to withdraw it and wire the money to a different account, often one overseas, keeping some of the money for themselves (ActionFraudUK, 2017). Sometimes they know the funds are crime proceeds; sometimes they are deceived into believing that the funds are genuine.

42 Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent.

criminalised by Member States. It aims at criminalising the intentional production, sale, procurement for use, import, distribution or otherwise making available of, for example, skimming devices used for stealing credentials, as well as malware and forged websites used for phishing. This Article is largely based on Article 4 of Framework Decision 2001/413/JHA and Article 3(d)(i) of Directive 2014/62/EU on the protection of the euro and other currencies against counterfeiting by criminal law.

Article 7: Incitement, aiding and abetting and attempt — this Article applies to conduct relating to the offences referred to in Articles 3 to 6 and requires Member States to criminalise all forms of preparation and participation. Criminal responsibility for attempt is included for the offences referred to in Articles 3 to 6.

Article 8: Penalties for natural persons — to effectively fight fraud and counterfeiting of non-cash means of payment, penalties have to be deterrent in all Member States. In line with other EU instruments approximating the level of criminal penalties, this Article stipulates that the maximum penalty under national law should be at least three years of imprisonment except for offences under Article 6, for which the maximum penalties should be at least two years. It provides for more severe penalties for aggravated offences, namely a maximum penalty of at least five years, where the crime is committed by a criminal organisation, as defined in Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime[43], or where a crime is conducted on a large scale, thus causing extensive or considerable damage, in particular including cases with low individual impact but high volume overall damage, or where a crime involves an aggregate advantage for the offender of at least EUR 20 000.

The offences listed in Articles 2 to 5 of Framework Decision 2001/413/JHA appear to be punishable by means of specific penalties in most of the Member States where information was available. However, in general, there is no approximation: while all Member States have penalties involving deprivation of liberty (at least in serious cases), the level of penalties for the same conduct varies significantly. Consequently, the deterrent effect is lower in some Member States than in others.

The disparities in the level of penalties may also impede judicial cooperation. If a Member State has low minimum penalties in its criminal code, this could lead law enforcement and judicial authorities to give low priority to investigating and prosecuting card-not-present fraud. This may in turn impede cross-border cooperation, when another Member State asks for assistance, in terms of timely processing of the request. Those who benefit most from such disparities in sanction levels are likely to be the most serious offenders, i.e. transnational organised crime groups with operative bases in several Member States.

Articles 9 and 10: Liability of and sanctions for legal persons — these Articles apply to all offences referred to in Articles 3 to 7. They require Member States to ensure liability of legal persons, without excluding the liability of natural persons, and to apply effective, proportionate and dissuasive sanctions to legal persons. Article 10 lists examples of sanctions.

Article 11: Jurisdiction — based on the principles of territoriality and personality, this Article lists situations in which Member States must establish jurisdiction for the offences referred to in Articles 3 to 7.

It has elements taken from Article 12 of Directive 2013/40/EU on attacks against information systems. In cases of fraud and counterfeiting of non-cash means of payment taking place online, the crime is likely to span several jurisdictions: it is often committed using information

[43] OJ L 300, 11.11.2008, p. 42.

systems outside the territory in which the offender is physically located and has consequences in another country where the evidence may also be located. Therefore, Article 11 aims at ensuring that territorial jurisdiction covers situations where the offender and the information system that the offender uses to commit the crime are located in different territories.

This Article includes a new element that addresses the need to assert jurisdiction if damage is caused in a jurisdiction other than that in which the conduct took place, including damage resulting from the theft of a person's identity. The aim is to cover situations not addressed in Directive 2013/40/EU on attacks against information systems, which are common to non-cash payment fraud crimes. These include cases in which none of the offences associated with the crime (e.g. stealing card credentials, cloning a card, unlawful withdrawal from an ATM) have been committed in the Member State where the damage occurs (e.g. where the victim has the bank account from which the money has been stolen). In these cases the victim is most likely to refer the incident to the authorities of the Member State in which the economic loss was detected. That Member State needs to be able to exercise jurisdiction to ensure effective investigation and prosecution, serving as the starting point for investigations that may involve multiple Member States and non-EU countries.

Article 12: Effective investigations — this Article aims at ensuring that the investigative tools provided for in national law for organised crime or other serious crime cases can also be used in cases of fraud and counterfeiting of non-cash means of payment, at least in serious cases. This Article also aims to ensure that, following lawful injunctions, information is provided to the authorities without undue delay.

Article 13: Exchange of information — this Article aims at encouraging greater use of operational national points of contact.

Article 14: Reporting of crime — this Article aims at addressing the need identified in the impact assessment to increase and facilitate reporting. It seeks to ensure the availability of appropriate channels for victims and private entities to report crimes, and to encourage reporting without undue delay in line with a similar provision under Article 16(2) of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography. Examples of actions to be undertaken are provided in Recital 19.

Article 15: Assistance and support to victims — this Article requires Member States to ensure that victims of non-cash payment fraud are offered information and channels to report a crime and advice on how to protect themselves against the negative consequences of fraud and against reputational damage arising from it.

This Article covers both natural and legal persons, which are also affected by the consequences of the offences covered by the proposal. It also introduces provisions to extend a number of specific rights established for natural persons under Directive 2012/29/EU to legal persons.

Article 16: Prevention — this Article addresses the need to raise awareness and thus reduce the risk of becoming a victim of fraud by means of information and awareness-raising campaigns, and research and education programmes. The impact assessment identified prevention gaps as a problem driver for non-cash payment fraud. This Article follows a similar approach to Article 23 (Prevention) of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography.

Article 17: Monitoring and statistics — this Article addresses the need to provide statistical data on fraud and counterfeiting of non-cash means of payment by making it obligatory for the Member States to ensure that an adequate system is in place for the recording, production and provision of statistical data on the offences referred to in the proposed directive, and on

monitoring the effectiveness of their systems (covering all judicial phases) to fight non-cash payment fraud. It follows a similar approach to Article 14 (Monitoring and statistics) of Directive 2013/40/EU on attacks against information systems, and Article 44 of Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (fourth Anti-Money Laundering Directive). It also aims to contribute to addressing the current limited availability of fraud data, which would assist in evaluating the effectiveness of national systems in fighting non-cash payment fraud.

Article 18: Replacement of Framework Decision 2001/413/JHA — this Article replaces the current provisions in the area of fraud and counterfeiting of non-cash means of payment, for Member States participating in this Directive.

Articles 19, 20, and 21 — these Articles contain further provisions on transposition by Member States, evaluation and reporting by the Commission and entry into force of the Directive.

2017/0226 (COD)

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 83(1) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee,

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Fraud and counterfeiting of non-cash means of payment is a threat to security, as it represents a source of income for organised crime and is therefore an enabler for other criminal activities such as terrorism, drug trafficking and trafficking in human beings.

(2) Fraud and counterfeiting of non-cash means of payment is also an obstacle to the digital single market, as it erodes consumers' trust and causes direct economic losses.

(3) Council Framework Decision 2001/413/JHA[44] needs to be updated and complemented by further provisions on offences, penalties and cross-border cooperation.

(4) Significant gaps and differences in Member States' laws in the area of fraud and counterfeiting of non-cash means of payment may hamper the fight against this type of crime and other serious and organised crimes related to and enabled by it, and may complicate effective police and judicial cooperation in this area.

(5) Fraud and counterfeiting of non-cash means of payment have a significant cross-border dimension, accentuated by an increasing digital component, which underlines the need for further action to approximate criminal legislation in this area.

(6) Recent years have brought not only an exponential increase in the digital economy but also a proliferation of innovation in many areas, including payment technologies. New payment technologies entail the use of new types of payment instruments, which, while creating new opportunities for consumers and businesses, also increase opportunities for fraud. Consequently, the legal framework must remain relevant and up-to-date against the background of these technological developments.

[44] Council Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment (OJ L 149, 2.6.2001, p. 1).

(7) Common definitions in this area are important to ensure a consistent approach in Member States' application of this Directive. The definitions need to cover new types of payment instruments, such as electronic money and virtual currencies.

(8) By giving the protection of the criminal law primarily to payment instruments that are provided with a special form of protection against imitation or abuse, the intention is to encourage operators to provide such special forms of protection to payment instruments issued by them, and thereby to add an element of prevention to the payment instrument.

(9) Effective and efficient criminal law measures are essential to protect non-cash means of payment against fraud and counterfeiting. In particular, a common criminal law approach is needed to the constituent elements of criminal conduct that contribute to or prepare the way for the actual fraudulent use of means of payment. Behaviour such as the collection and possession of payment instruments with the intention to commit fraud, through, for instance, phishing or skimming, and their distribution, for example by selling credit card information on the internet, should thus be made a criminal offence in its own right without being directly linked to the actual fraudulent use of means of payment. So such criminal conduct should also cover circumstances where possession, procurement or distribution does not necessarily lead to fraudulent use of such payment instruments, if the offender is aware of such a possibility (*dolus eventualis*). This Directive does not sanction the legitimate use of a payment instrument, including and in relation to the provision of innovative payment services, such as services commonly developed by fintech companies.

(10) The sanctions and penalties for fraud and counterfeiting of non-cash means of payment should be effective, proportionate and dissuasive throughout the Union.

(11) It is appropriate to provide for more severe penalties where the crime is committed by a criminal organisation, as defined in Council Framework Decision 2008/841/JHA[45], or where a crime is conducted on a large scale, thus involving extensive or considerable damage to the victims or an aggregate advantage for the offender of at least EUR 20 000.

(12) Jurisdictional rules should ensure that the offences laid down in this Directive are prosecuted effectively. In general, offences are best dealt with by the criminal justice system of the country in which they occur. Member States should therefore establish their jurisdiction over offences committed on their territory, over offences committed by their nationals and over offences that cause damage in their territory.

(13) Information systems challenge the traditional concept of territoriality because in principle they can be used and controlled remotely from anywhere. Where Member States assert jurisdiction on the basis of offences committed within their territory, it appears appropriate to assess the scope of their jurisdiction for offences committed using information systems as well. Jurisdiction in such cases should cover situations where the information system is located within the territory of the Member State although the offender may be located outside of it and situations where the offender is located within the territory of the Member State although the information system may be located outside of it.

---

45 Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime (OJ L 300, 11.11.2008, p. 42).

(14) The complexity of assigning jurisdiction with regard to the effects of the offence in a different jurisdiction from that in which the actual act took place needs to be addressed. Jurisdiction should thus be asserted for offences committed by offenders irrespective of their nationality and physical presence, but in view of any damage caused by such an act on the territory of the Member State.

(15) Given the need for special tools to effectively investigate fraud and counterfeiting of non-cash means of payment, and their relevance for effective international cooperation between national authorities, investigative tools that are typically used for cases involving organised crime and other serious crime should be available to competent authorities in all Member States for the investigation of such offences. Taking into account the principle of proportionality, the use of such tools in accordance with national law should be commensurate with the nature and gravity of the offences under investigation. In addition, law enforcement authorities and other competent authorities should have timely access to relevant information in order to investigate and prosecute the offences laid down in this Directive.

(16) In many cases, criminal activities underlie incidents that should be notified to the relevant national competent authorities under Directive (EU) 2016/1148 of the European Parliament and the Council[46]. Such incidents may be suspected to be of criminal nature even if the evidence of a criminal offence is not sufficiently clear from the outset. In this context, relevant operators of essential services and digital service providers should be encouraged to share the reports required under Directive (EU) 2016/1148 with law enforcement authorities so as to form an effective and comprehensive response and to facilitate attribution and accountability by the perpetrators for their actions. In particular, promoting a safe, secure and more resilient environment requires systematic reporting of incidents of a suspected serious criminal nature to law enforcement authorities. Moreover, when relevant, Computer Security Incident Response Teams designated under Article 9 of Directive (EU) 2016/1148 should be involved in law enforcement investigations with a view to providing information, as considered appropriate at national level, and also providing specialist expertise on information systems.

(17) Major security incidents as defined in Article 96 of Directive (EU) 2015/2366 of the European Parliament and the Council[47] may be of criminal origin. Where relevant, payment service providers should be encouraged to share with law enforcement authorities the reports they are required to submit to the competent authority in their home Member State under Directive (EU) 2015/2366.

(18) A number of instruments and mechanisms exist at Union level to enable the exchange of information among national law enforcement authorities to investigate and prosecute crimes. To facilitate and speed up cooperation among national law enforcement authorities and make sure that those instruments and mechanisms are used to their fullest extent, this Directive should strengthen the importance of the operational points of contact introduced by Council Framework Decision

[46] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

[47] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

2001/413/JHA. Member States may decide to make use of the existing network of operational points of contact, such as that set up in Directive 2013/40/EU of the European Parliament and of the Council[48]. They should provide effective assistance, for example facilitating the exchange of relevant information and the provision of technical advice or legal information. To ensure the network runs smoothly, each point of contact should be able to communicate quickly with the point of contact of another Member State. Given the significant trans-border dimension of this area of crime and in particular the volatile nature of the electronic evidence, Member States should be able to promptly deal with urgent requests from this network of points of contact and provide feedback within eight hours.

(19) Reporting crime without undue delay to public authorities is of great importance in combating fraud and counterfeiting of non-cash means of payment, as it is often the starting point of the criminal investigation. Measures should be taken to encourage reporting by natural and legal persons, in particular financial institutions to law enforcement and judicial authorities. These measures can be based on various types of action, including legislative ones, such as obligations to report suspected fraud, or non-legislative ones, such as setting up or supporting organisations or mechanisms favouring the exchange of information, or awareness raising. Any such measure that involves processing of the personal data of natural persons should be carried out in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[49]. In particular, any transmission of information regarding preventing and combating offences relating to fraud and counterfeiting of non-cash means of payment should comply with the requirements laid down in Regulation (EU) 2016/679, notably the lawful grounds for processing.

(20) Fraud and counterfeiting of non-cash means of payment can result in serious economic and non-economic consequences for its victims. Where such fraud involves identity theft, its consequences are often aggravated because of reputational damage and serious emotional harm. Member States should adopt measures of assistance, support and protection aimed at mitigating these consequences.

(21) Natural persons who are victims of fraud related to non-cash means of payment have rights conferred under Directive 2012/29/EU of the European Parliament and the Council[50]. Member States should adopt measures of assistance and support to such victims which build on the measures required by Directive 2012/29/EU but respond more directly to the specific needs of victims of fraud related to identity theft. Such measures should include, in particular, specialised psychological support and advice on financial, practical and legal matters, as well as assistance in receiving available compensation. Specific information and advice on protection against the negative consequences of such crime should be offered to legal persons as well.

---

48 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

49 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

50 Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA (OJ L 315, 14.11.2012, p. 57).

(22) This Directive should provide for the right for legal persons to access information about the procedures for making complaints. This right is necessary in particular for small and medium-sized enterprises[51] and should contribute to creating a friendlier business environment for small and medium-sized enterprises. Natural persons already benefit from this right under Directive 2012/29/EU.

(23) Member States should establish or strengthen policies to prevent fraud and counterfeiting of non-cash means of payment, and measures to reduce the risk of becoming victims of such offences, by means of information and awareness-raising campaigns and research and education programmes.

(24) There is a need to collect comparable data on the offences laid down in this Directive. Relevant data should be made available to the competent specialised Union agencies and bodies, such as Europol, in line with their tasks and information needs. The aim would be to gain a more complete picture of the problem of fraud and counterfeiting of non-cash means of payment and issues relating to payment security at Union level, and so contribute to formulating a more effective response. Member States should make full use of Europol's mandate and capacity to provide assistance and support to relevant investigations, by submitting information on the offenders' *modus operandi* to Europol for the purpose of conducting strategic analyses and threat assessments of fraud and counterfeiting of non-cash means of payment in accordance with Regulation (EU) 2016/794 of the European Parliament and of the Council[52]. Providing information can help better understand present and future threats and assist the Council and the Commission in laying down strategic and operational priorities of the Union for fighting crime and in the ways of implementing those priorities.

(25) This Directive aims to amend and expand the provisions of Council Framework Decision 2001/413/JHA. Since the amendments to be made are substantial in number and nature, Framework Decision 2001/413/JHA should, in the interests of clarity, be replaced in its entirety for Member States bound by this Directive.

(26) In accordance with Article 3 of the Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, those Member States have notified their wish to take part in the adoption and application of this Directive.

OR

(26) In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, the United Kingdom has notified [, by letter of …,] its wish to take part in the adoption and application of this Directive.

OR

---

51 Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

52 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

(26) In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Ireland has notified [, by letter of …,] its wish to take part in the adoption and application of this Directive.

AND/OR

(26) In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, those Member States are not taking part in the adoption of this Directive and are not bound by it or subject to its application.

OR

(26) In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Directive and is not bound by it or subject to its application.

OR

(26) In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, the United Kingdom is not taking part in the adoption of this Directive and is not bound by it or subject to its application.

(27) In accordance with Articles 1 and 2 of the Protocol No 22 on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Directive and is not bound by it or subject to its application.

(28) Since the objectives of this Directive, namely to subject fraud and counterfeiting of non-cash means of payment to effective, proportionate and dissuasive criminal penalties and to improve and encourage cross-border cooperation both between competent authorities and between natural and legal persons and competent authorities, cannot be sufficiently achieved by the Member States, and can therefore, by reason of their scale or effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(29) This Directive respects fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, including the right to liberty and security, the respect for private and family life, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy and to a fair trial, the presumption of innocence and right of defence, the principles of the legality and proportionality of criminal offences and penalties, as well as the right not to be tried or punished twice in criminal proceedings for the same

criminal offence. This Directive seeks to ensure full respect for those rights and principles and should be implemented accordingly,

HAVE ADOPTED THIS DIRECTIVE:

TITLE I: SUBJECT MATTER AND DEFINITIONS

Article 1
Subject matter

This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of fraud and counterfeiting of non-cash means of payment.

Article 2
Definitions

For the purpose of this Directive, the following definitions shall apply:

(a) 'payment instrument' means a protected device, object or record, other than legal tender, which, alone or with a procedure or a set of procedures, enables the holder or user to transfer money or monetary value or to initiate a payment order, including by means of digital mediums of exchange;

(b) 'protected device, object or record' means a device, object or record safeguarded against imitation or fraudulent use, for example through design, coding or signature;

(c) 'payment order' means a payment order as defined in point (13) of Article 4 of Directive (EU) 2015/2366;

(d) 'digital medium of exchange' means any electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council[53], and virtual currencies;

(e) 'virtual currencies' means a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically;

(f) 'payment service' means a payment service as defined in point (3) of Article 4 of Directive (EU) 2015/2366;

(g) 'payment service user' means a payment service user as defined in point (10) of Article 4 of Directive (EU) 2015/2366;

(h) 'payment account' means a payment account as defined in point (12) of Article 4 of Directive (EU) 2015/2366;

(i) 'payment transaction' means a payment transaction as defined in point (5) of Article 4 of Directive (EU) 2015/2366;

[53] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).

(j) ‘payer’ means a natural or legal person, who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order or transfers virtual currency;

(k) ‘payee’ means a payee as defined in point (9) of Article 4 of Directive (EU) 2015/2366;

(l) ‘information system’ means information system as defined in point (a) of Article 2 of Directive 2013/40/EU;

(m) ‘computer data’ computer data as defined in point (b) of Article 2 of Directive 2013/40/EU.

TITLE II: OFFENCES

Article 3
Fraudulent use of payment instruments

Member States shall take the necessary measures to ensure that, when committed intentionally, the following are punishable as a criminal offence:

(a) fraudulent use of a stolen or otherwise unlawfully appropriated payment instrument;

(b) fraudulent use of a counterfeited or falsified payment instrument.

Article 4
Offences preparatory to the fraudulent use of payment instruments

Member States shall take the necessary measures to ensure that, when committed intentionally, the following are punishable as a criminal offence:

(a) theft or other unlawful appropriation of a payment instrument;

(b) counterfeiting or falsification of a payment instrument in order for it to be used fraudulently;

(c) possession, procurement for use, import, export, sale, transport, distribution or otherwise making available of a stolen or otherwise unlawfully appropriated, or of a counterfeited or falsified payment instrument in order for it to be used fraudulently.

Article 5
Offences related to information systems

Member States shall take the necessary measures to ensure that performing or causing a transfer of money, monetary value or virtual currencies in order to make an unlawful gain for the perpetrator or a third party is punishable as a criminal offence, when committed intentionally by:

(a) hindering or interfering with the functioning of an information system;

(b) introducing, altering, deleting, transmitting or suppressing computer data.

Article 6
Tools used for committing offences

Member States shall take the necessary measures to ensure that, when committed intentionally with fraudulent purpose, the production, procurement for use, import, export, sale, transport, distribution or otherwise making available of a device or an instrument, computer data or any other means specifically designed or adapted for the purpose of committing any of the offences referred to in Article 4(a) and (b) or Article 5, is punishable as a criminal offence.

Article 7
Incitement, aiding and abetting and attempt

1. Member States shall take the necessary measures to ensure that inciting or aiding and abetting an offence referred to in Articles 3 to 6 is punishable as a criminal offence.

2. Member States shall take the necessary measures to ensure that the attempt to commit an offence referred to in Articles 3 to 6 is punishable as a criminal offence.

Article 8
Penalties for natural persons

1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by effective, proportionate and dissuasive criminal penalties.

2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3, 4 and 5 are punishable by a maximum term of imprisonment of at least three years.

3. Member States shall take the necessary measures to ensure that the offences referred to in Article 6 are punishable by a maximum term of imprisonment of at least two years.

4. Member States shall take the necessary measures to ensure that offences referred to in Articles 3, 4 and 5 are punishable by a maximum term of imprisonment of at least five years if:

   (a) they are committed within the framework of a criminal organisation, as defined in Framework Decision 2008/841/JHA, irrespective of the penalty provided for in that Decision;

   (b) they involve extensive or considerable damage or an aggregate advantage of at least EUR 20 000.

Article 9
Liability of legal persons

1. Member States shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 3 to 7 committed for their benefit by any person, acting either individually or as part of an organ of the legal person, and having a leading position within the legal person, based on one of the following:

   (a) a power of representation of the legal person;

   (b) an authority to take decisions on behalf of the legal person;

   (c) an authority to exercise control within the legal person.

2. Member States shall take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission, by a person under its authority, of any of the offences referred to in Articles 3 to 7 for the benefit of that legal person.

3. Liability of legal persons under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators or inciters of, or accessories to, any of the offences referred to in Articles 3 to 7.

Article 10
Sanctions for legal persons

Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 9(1) is subject to effective, proportionate and dissuasive sanctions, which shall include criminal or non-criminal fines and which may include other sanctions, such as:

(a) exclusion from entitlement to public benefits or aid;

(b) temporary or permanent disqualification from the practice of commercial activities;

(c) placing under judicial supervision;

(d) judicial winding-up;

(e) temporary or permanent closure of establishments which have been used for committing the offence.

TITLE III: JURISDICTION AND INVESTIGATION

Article 11
Jurisdiction

1. Each Member State shall take the necessary measures to establish its jurisdiction over the offences referred to in Articles 3 to 7 where:

   (a) the offence is committed in whole or in part in its territory;

   (b) the offender is one of its nationals;

   (c) the offence causes damage in its territory including damage resulting from the theft of the identity of a person.

2. When establishing jurisdiction in accordance with point (a) of paragraph 1, a Member State shall ensure that it has jurisdiction where:

   (a) the offender commits the offence when physically present on its territory, whether or not the offence is committed using computers or an information system on its territory;

   (b) the offence is committed using computers or an information system on its territory, whether or not the offender commits the offence when physically present on its territory.

3. A Member State shall inform the Commission if it decides to establish jurisdiction over an offence referred to in Articles 3 to 7 committed outside its territory, including where:

   (a) the offender has his or her habitual residence in its territory;

(b) the offence is committed for the benefit of a legal person established in its territory;

(c) the offence is committed against one of its nationals or a person who is an habitual resident in its territory.

Article 12
Effective investigations

1. Member States shall take the necessary measures to ensure that effective investigative tools, such as those which are used in organised crime or other serious crime cases, are available to persons, units or services responsible for investigating or prosecuting the offences referred to in Articles 3 to 7.

2. Member States shall take the necessary measures to ensure that, where national law oblige natural and legal persons to submit information regarding offences referred to in Articles 3 to 7, such information reaches the authorities investigating or prosecuting those offences without undue delay.

TITLE IV: EXCHANGE OF INFORMATION AND REPORTING OF CRIME

Article 13
Exchange of information

1. For the purpose of exchanging information relating to the offences referred to in Articles 3 to 7, Member States shall ensure that they have an operational national point of contact available 24 hours a day and seven days a week. Member States shall also ensure that they have procedures in place so that urgent requests for assistance are promptly dealt with and the competent authority replies within eight hours of receipt, at least indicating whether the request will be answered, and the form and estimated time of such an answer. Member States may decide to make use of the existing networks of operational points of contact.

2. Member States shall inform the Commission, Europol and Eurojust of their appointed point of contact referred to in paragraph 1. The Commission shall forward that information to the other Member States.

Article 14
Reporting of crime

1. Member States shall take the necessary measures to ensure that appropriate reporting channels are made available in order to facilitate reporting of the offences referred to in Articles 3 to 7 to law enforcement and other competent national authorities without undue delay.

2. Member States shall take the necessary measures to encourage financial institutions and other legal persons operating in their territory to report without undue delay suspected fraud to law enforcement and other competent authorities, for the purpose of detecting, preventing, investigating or prosecuting offences referred to in Articles 3 to 7.

TITLE V: ASSISTANCE TO VICTIMS AND PREVENTION

Article 15
Assistance and support to victims

1. Member States shall ensure that natural and legal persons who have suffered a prejudice from offences referred to in Articles 3 to 7, committed by misusing personal data, are offered specific information and advice on how to protect themselves against the negative consequences of the offences, such as reputational damage.

2. Member States shall ensure that legal persons that are victims of offences referred to in Articles 3 to 7 of this Directive are, without undue delay after their first contact with a competent authority, offered information about:

   (a) the procedures for making complaints with regard to the offence and their role in connection with such procedures;

   (b) the available procedures for making complaints if the competent authority does not respect their rights in the course of criminal proceedings;

   (c) the contact details for communications about their case.

Article 16
Prevention

Member States shall take appropriate action, including through the Internet, such as information and awareness-raising campaigns, research and education programmes, where appropriate in cooperation with stakeholders, aimed at reducing overall fraud, raising awareness and reducing the risk of becoming a victim of fraud.

TITLE VI: FINAL PROVISIONS

Article 17
Monitoring and statistics

1. By [3 months after entry into force of this Directive] at the latest, the Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Directive. The monitoring programme shall set out the means by which and the intervals at which the data and other necessary evidence will be collected. It shall specify the action to be taken by the Commission and by the Member States in collecting, sharing and analysing the data and other evidence.

2. Member States shall ensure that a system is in place for the recording, production and provision of statistical data measuring the reporting, investigative and judicial phases concerning the offences referred to in Articles 3 to 7.

3. The statistical data referred to in paragraph 2 shall, as a minimum, cover the number of offences referred to in Articles 3 to 7 reported to the Member States, the number of cases investigated, the number of persons prosecuted for and convicted of the offences referred to in Articles 3 to 7, and data on the functioning of the reporting, investigative and judicial phases concerning these offences.

4. Member States shall transmit the data collected pursuant to paragraphs 1, 2 and 3 to the Commission on an annual basis. The Commission shall ensure that a consolidated review of the statistical reports is published each year and submitted to the competent specialised Union agencies and bodies.

Article 18
Replacement of Framework Decision 2001/413/JHA

Framework Decision 2001/413/JHA is replaced with regard to Member States bound by this Directive, without prejudice to the obligations of those Member States with regard to the date for transposition of that Framework Decision into national law.

With regard to Member States bound by this Directive, references to Framework Decision 2001/413/JHA shall be construed as references to this Directive.

Article 19
Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by [24 months after entry into force]. They shall immediately inform the Commission thereof.
2. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such a reference shall be laid down by the Member States.
3. Member States shall communicate to the Commission the text of measures that they adopt in the field covered by this Directive.

Article 20
Evaluation and reporting

1. The Commission shall, by [48 months after entry into force], submit a report to the European Parliament and the Council, assessing the extent to which the Member States have taken the necessary measures in order to comply with this Directive. Member States shall provide the Commission with necessary information for the preparation of the report.
2. The Commission shall, by [96 months after entry into force], carry out an evaluation of this Directive on combating fraud and counterfeiting of non-cash means of payment and submit a report to the European Parliament and to the Council.

Article 21
Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Brussels,

For the European Parliament
The President

For the Council
The President