



Brussels, 18 December 2018
(OR. en)

15695/18

Interinstitutional File:
2017/0226(COD)

DROIPEN 217
CYBER 331
JAI 1318
TELECOM 492
MI 1014
CODEC 2382

'I' ITEM NOTE

From: Presidency
To: Permanent Representatives Committee (Part 2)
Subject: 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

1. On 13 September 2017, the Commission submitted a 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.
2. The Council reached a general approach on the draft text under Bulgarian Presidency in March 2018 (6472/1/18 REV 1).

3. The LIBE Committee of the European Parliament adopted its report on 3 September, which was endorsed at the plenary meeting on 12 September 2018. On this basis, the Austrian Presidency, acting on behalf of the Council, conducted trilogue negotiations with the European Parliament and the Commission with a view to reaching an agreement in first reading.
4. On 11 December 2018, a provisional agreement was reached at the fourth trilogue, which resulted in the final compromise text set out in the Annex to this note.
5. In the light of the above, the Permanent Representatives Committee is invited to:
 - a) approve the final compromise text regarding the 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, as set out in the Annex to this note; and
 - b) confirm that the Presidency can indicate to the European Parliament that, should the European Parliament at first reading adopt its position concerning the Directive as set out in the Annex to this note, subject, if necessary, to revision of this text by the lawyer-linguists of both institutions, the Council would approve the European Parliament's position and the act shall be adopted in the wording which corresponds to the European Parliament's position.

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/JHA¹ needs to be updated and complemented in order to include further provisions on offences, in particular relating to computer-related fraud, penalties, prevention and assistance to victims 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 obstruct the prevention, detection and sanctioning of this type of crime and other serious and organised crimes related to and enabled by it, and complicate effective police and judicial cooperation in this area with an impact on security.

- (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 on the basis of a technology-neutral approach.
- (6a) This Directive applies to non-cash payment instruments only insofar as the instrument's payment function is concerned.
- (6aa) The use of new types of payment instruments creates opportunities for consumers and businesses but also increases opportunities for fraud. Fraud is not only used to fund criminal groups, it also limits the development of the digital single market and makes citizens more reluctant to make online purchases.
- (7) Common definitions in this area are important to ensure a consistent approach in Member States' application of this Directive and to facilitate information exchange and cooperation between competent authorities. The definitions need to cover new types of non-cash payment instruments which allow for transfers of electronic money and virtual currencies. The definition of non-cash payment instruments should acknowledge that a non-cash payment instrument may consist of different elements acting together, as for example a mobile payment application and a corresponding authorization (e.g. a password). When this Directive uses the notion of a non-cash payment instrument, it is understood that the instrument puts the holder or user of the instrument in the position to actually enable a transfer of money or monetary value or to initiate a payment order. For example, unlawful obtention of a mobile payment application without the necessary authorization would not be considered an unlawful obtention of a non-cash payment instrument as it does not actually enable the user to transfer money or monetary value.

- (7a) This Directive covers virtual currencies only insofar as they can be commonly used for making payments. The Member States are encouraged to ensure in their national law that future currencies of a virtual nature issued by their central banks or other public authorities will enjoy the same level of protection against fraudulent offences as non-cash means of payment in general. Digital wallets that allow transferring virtual currencies should be covered by this Directive to the same extent as non-cash payment instruments. The inclusion of digital mediums of exchange in the definitions acknowledges that digital wallets for transferring virtual currencies may provide, but do not necessarily provide the features of a payment instrument and does not extend the definition of a payment instrument.
- (7aa) Sending fake invoices with which payment credentials can be abstracted should be considered as an attempt at unlawful appropriation as referred to in this Directive.
- (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, skimming or directing or redirecting payment service users to imitation websites, 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 requiring 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. However, where this Directive criminalizes possession or holding, such criminalization does not encompass mere omission. 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.

- (9a) With regard to the criminal offences provided for in this Directive, the notion of intention apply to all elements constituting those criminal offences in accordance with national law. The intentional nature of an act, as well as knowledge or purpose required as an element of an offence, may be inferred from objective, factual circumstances. Criminal offences which do not require intention are not covered by this Directive.
- (9b) This Directive refers to classical forms of conduct, like fraud, forgery, theft and unlawful appropriation that have been shaped by national law already before the era of digitalization. The extended scope of the Directive with regard to non-corporeal payment-instruments therefore requires defining equivalent forms of conduct in the digital sphere, complementing and reinforcing Directive 2013/40¹. Unlawful obtaining of a non-corporeal non-cash payment instrument should be a criminal offence, at least when this obtaining has involved the commission of one of the offences referred to in Articles 3 to 6 of Directive 2013/40 or misappropriation of a non-corporeal non-cash payment instrument. 'Misappropriation' means the action of a person, who is entrusted with a non-corporeal non-cash payment instrument, to knowingly use the instrument without right to his own benefit or to the benefit of another. Procurement for fraudulent use of such an unlawfully obtained instrument should be punishable, without it being necessary to establish all the factual elements of the unlawful obtaining, let alone require a prior or simultaneous conviction for the predicate offence which generated the unlawful obtaining.
- (9c) The Directive also refers to tools which can be used in order to commit the offences referred to in this Directive. Motivated by the need to avoid criminalization where such tools are produced and put to the market for legitimate purposes and are therefore, though sometimes used to commit criminal offences, not in themselves a threat, criminalization is limited to tools which are primarily designed or specifically adapted for the purpose of committing the offences referred to in this Directive.

¹ 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).

- (10) The sanctions and penalties for fraud and counterfeiting of non-cash means of payment should be effective, proportionate and dissuasive throughout the Union. This Directive is without prejudice to the individualisation and application of penalties and execution of sentences in accordance with the circumstances of the case and the general rules of national criminal law.
- (10a) As this Directive provides for minimum rules, Member States are free to adopt or maintain more stringent criminal law rules with regard to fraud and counterfeiting of non-cash means of payment, including a broader definition of offences.
- (11) It is appropriate to provide for more severe penalties where the crime is committed in the framework of a criminal organisation, as defined in Council Framework Decision 2008/841/JHA², Member States should not be obliged to provide for specific aggravating circumstances where national law provides for separate criminal offences and this may lead to more severe sanctions. When an offence referred to in this Directive has been committed, by the same person, in conjunction with another offence referred to in this Directive, which de facto constitutes a necessary element of the first offence, a Member State may, in accordance with general principles of national law, provide that such conduct is regarded as an aggravating circumstance to the main offence.
- (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. Member States may also establish their jurisdiction over offences that cause damage in their territory and are strongly encouraged to do so.

² Council Framework Decision 2008/841/JHA of October 2008 on the fight against organised crime (OJ L 300, 11.11.2008, p. 42).

- (12a) Recalling the obligations under Framework Decision 2009/948³ and Decision 2002/187/JHA⁴, competent authorities are encouraged to use in cases of conflicts of jurisdiction the possibility to conduct direct consultations with the assistance of Eurojust.
- (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, if and to the extent that the use of those tools is appropriate and commensurate with the nature and gravity of the offences as defined in national law. 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. Member States are encouraged to allocate adequate human and financial resources to the competent authorities in order to properly investigate and prosecute the offences laid down in this Directive.
- (15a) National authorities investigating or prosecuting offences referred to in Articles 3 to 7 should be empowered to cooperate with other national authorities and their counterparts in other Member States.

³ Council Framework Decision 2009/948 of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (OJ L 328, 15.12.2009, p. 42).

⁴ Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63, 6.3.2002, p. 1).

- (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. 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 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 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. 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. In very urgent and serious cases, Member States should inform Europol.

- (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. 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.
- (19bis) In order to facilitate the immediate reporting of crime, the Commission should carefully assess the establishment of effective online fraud-reporting systems by Member States and standardised reporting templates at Union level. Such systems could facilitate the immediate reporting of non-cash fraud which often takes place online and therefore strengthen the support for victims, the identification and analysis of cybercrime threats to citizens and legal persons and the work and cross-border cooperation of national competent authorities.
- (19a) The offences envisaged in the Directive often have a cross-border nature. Therefore, combating these offences relies on the close cooperation between the Member States. Member States are encouraged to ensure, to the extent appropriate, effective application of mutual recognition and legal assistance instruments in relation to the offences covered by the Directive.

- (19 aa) Investigation and prosecution of all types of fraud and counterfeiting of non-cash means of payment, including those involving small amounts of money, are particularly important in order to proactively combat that phenomenon. Reporting obligations, information exchange and statistical reports are efficient ways to detect fraudulent activities, especially similar activities that involve small amounts of money when considered separately.
- (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, for example, identity theft, its consequences are often aggravated because of reputational and professional damage, damage to an individual's credit rating as well as serious emotional harm. Member States should adopt measures of assistance, support and protection aimed at mitigating these consequences.
- (20 a) It often takes a considerable amount of time for victims to find out that they have suffered a loss from fraud and counterfeiting offences. During this time a spiral of interlinked crimes might develop, thereby aggravating the negative consequences for the victims.
- (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. 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, the provision of a list of dedicated institutions covering different aspects of identity-related crime and victim support, specialised psychological support and advice on financial, practical and legal matters, as well as assistance in receiving available compensation. Member States should also be able to set up a national single online information tool to facilitate access to assistance and support for victims. Specific information and advice on protection against the negative consequences of such crime should be offered to legal persons as well.

- (22) This Directive should provide for the right for legal persons to access information in accordance with national law about the procedures for making complaints. This right is necessary in particular for small and medium-sized enterprises⁵ 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, assisted by the Commission, 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, permanent online information tools with practical examples of fraudulent practices and research and education programmes. Special attention should be paid in particular to the needs and interests of vulnerable persons. Member States are encouraged to ensure that sufficient funding is made available for such campaigns.
- (23b) Member States should develop and keep up to date, as part of the information campaigns referred to in Article 16 permanent online information tool with practical examples of fraudulent practices as referred to in Articles 3 to 7 in a format that is easy to understand. This tool may be linked to or be part of the single online information tool referred to in Article 15(1b).

⁵ Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

- (24) It is necessary to collect statistical data on fraud and counterfeiting of non-cash payment instrument, and Member States should therefore be obliged to ensure that an adequate system is in place for the recording, production and provision of existing statistical data on the offences referred to in the proposed Directive.
- (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 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.
- (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.

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. It facilitates the prevention of such offences, and assisting and supporting of victims.

Article 2

Definitions

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

- (a) ‘non-cash payment instrument’ means a non-corporeal or corporeal protected device, object or record, or a combination thereof, other than legal tender, which, alone or in conjunction with a procedure or a set of procedures, enables the holder or user to transfer money or monetary value, 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) ‘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, and virtual currencies;

- (d) ‘virtual currencies’ means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically;
- (e) ‘information system’ means information system as defined in point (a) of Article 2 of Directive 2013/40/EU;
- (f) ‘computer data’ computer data as defined in point (b) of Article 2 of Directive 2013/40/EU;
- (g) 'legal person' means an entity having legal personality under the applicable law, except for States or public bodies in the exercise of State authority and for public international organisations.

**TITLE II:
OFFENCES**

Article 3

Fraudulent use of non-cash payment instruments

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

- (a) fraudulent use of a stolen or otherwise unlawfully appropriated or obtained non-cash payment instrument;
- (b) fraudulent use of a counterfeited or falsified non-cash payment instrument.

Article 4

Offences related to the fraudulent use of corporeal non-cash payment instruments

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

- (a) theft or other unlawful appropriation of a corporeal non-cash payment instrument;
- (b) fraudulent counterfeiting or falsification of a corporeal non-cash payment instrument;
- (c) possession of a stolen or otherwise unlawfully appropriated, or of a counterfeited or falsified corporeal non-cash payment instrument for fraudulent use;
- (d) procurement for oneself or another, including receiving, appropriation, buying, transfer, import, export, sale, transport and distribution of a stolen, counterfeited or falsified corporeal non-cash payment instrument for fraudulent use.

Article 4a

Offences related to the fraudulent use of non-corporeal non-cash payment instruments

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

- (a) unlawful obtaining of a non-corporeal non-cash payment instrument, at least when this obtaining has involved the commission of one of the offences referred to in Article 3 to 6 of Directive 2013/40, or misappropriation of a non-corporeal non-cash payment instrument;
- (b) fraudulent counterfeiting or falsification of a non-corporeal non-cash payment instrument;
- (c) holding of an unlawfully obtained, falsified or counterfeited non-corporeal non-cash payment instrument for fraudulent use, at least if the unlawful origin is known at the time of the holding of the instrument;
- (d) procurement for oneself or another, including sale, transfer and distribution, or making available, of an unlawfully obtained, falsified or counterfeited non-corporeal non-cash payment instrument for fraudulent use.

Article 5

Fraud 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 and thereby causing an unlawful loss of property for another person 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) without right hindering or interfering with the functioning of an information system;
- (b) without right 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 the producing, procurement for oneself or another, including import, export, sale, transport and distribution, or making available of a device or an instrument, computer data or any other means primarily designed or specifically adapted for the purpose of committing any of the offences referred to in Article 4(a), 4(b), 4a(a), 4a(b) or Article 5, at least when committed with the intention that these means be used, 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, 4 (a), 4 (b), 4 (d), 4a (a), 4a (b), and 5 is punishable as a criminal offence. With regard to Article 4a (d), Member States shall take the necessary measures to at least ensure that attempted fraudulent procurement for oneself or another 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(a), 4(b), 4a(a) and 4a(b) are punishable by a maximum term of imprisonment of at least two-years.
3. Member States shall take the necessary measures to ensure that the offence referred in Article 5 is punishable by a maximum term of imprisonment of at least three-years.
4. Member States shall take the necessary measures to ensure that the offences referred to in Articles 4 (c), 4(d), 4a (c) and 4a(d) are punishable by a maximum term of imprisonment of at least one year.

5. Member States shall take the necessary measures to ensure that the offence referred to in Article 6 is punishable by a maximum term of imprisonment of at least two years.
6. 4. Member States shall take the necessary measures to ensure that offences referred to in Articles 3, 4, 4a and 5 are punishable by a maximum term of imprisonment of at least five years if 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.

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) or 9(2) 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;
- (a a) temporary exclusion from access to public funding, including tender procedures, grants and concessions;
- (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.
2. When establishing jurisdiction in accordance with point (a) of paragraph 1, a Member State shall ensure that it has jurisdiction where the offender commits the offence when physically present on its territory, whether or not the offence is committed using an information system 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 and cooperation

1. Member States shall take the necessary measures to ensure that investigative tools, such as those which are used in countering organised crime or other serious crime cases, are effective, proportionate to the crime committed and 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 and update that information as necessary. 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.

Article 15

Assistance and support to victims

1. Member States shall ensure that natural and legal persons who have suffered 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,
 - 1 a. Member States shall ensure that natural and legal persons who have suffered prejudice from offences referred to in Articles 3 to 7, committed by misusing personal data, are provided with a list of dedicated institutions that deal with different aspects of identity-related crime and support.
 - 1 b. Member States are encouraged to set up national single online information tools to facilitate access to assistance and support for natural or legal persons who have suffered prejudice from offences referred to in Articles 3 to 7, committed by misusing personal data.
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;
 - (aa) the right of receiving information about the case in accordance with national law;
 - (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.

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 anonymised 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 existing data on the number of offences referred to in Articles 3 to 7 registered by the Member States, and the number of persons prosecuted for and convicted of the offences referred to in Articles 3 to 6.
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 84 months after entry into force, carry out an evaluation of this Directive on combating fraud and counterfeiting of non-cash means of payment, as well as its impact on fundamental rights, and submit a report to the European Parliament and to the Council. Member States shall provide the Commission with necessary information for the preparation of the report.
 - 2a. In the context of the evaluation referred to in paragraph 2, the Commission shall also report on the necessity, the feasibility and the effectiveness of creating national secure online systems to allow victims to report any of the offences referred to in Articles 3 to 7, as well as of establishing a standardised Union reporting template that shall serve as a basis for Member States.

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.